Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado

Facultad de Ingeniería de Sistemas e Informática

Unidad de Posgrado

Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001

TESIS

Para optar el Grado Académico de Magíster en Gobierno de Tecnologías de Información

AUTOR

Javier Alfonso SECLÉN ARANA

ASESOR

Rómulo Fernando LOMPARTE ALVARADO

Lima, Perú

2016

Referencia bibliográfica

Seclen, J. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001*. [Tesis de maestría, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú, DECANA DE AMERICA
Facultad de Ingeniería de Sistemas e Informática
UNIDAD DE POSGRADO

SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN

En la Ciudad Universitaria, a los Veintisiete (27) días del mes de mayo del 2016, siendo las 20:30 horas, se reunieron en el Aula Magna de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos, el Jurado Examinador de tesis conformado por los siguientes profesores:

Dra. Nora Bertha La Serna Palomino (Presidente).
Mg. Rómulo Fernando Lomparte Alvarado (Miembro Asesor).
Mg. Julio César Rojas Medina (Miembro).
Dra. Luz Sussy Bayona Oré (Miembro).
Mg. Ciro Aguilar Linares (Miembro).

Se inició la Sustentación de la tesis invitando al graduando ***Javier Alfonso Seclén Arana****, para que realizara la exposición oral y pública de la tesis para optar el Grado Académico de Magíster en Gobierno de Tecnologías de Información, siendo la Tesis intitulada:*

"Factores que Afectan la Implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas Peruanas de Acuerdo a la NTP-ISO/IEC 27001"

Concluida la exposición, los miembros del Jurado Examinador procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

18 DIECIOCHO MUY BUENO

Por tanto el Presidente del Jurado, de acuerdo al Reglamento de Grados y Títulos, le otorga al bachiller ***Javier Alfonso Seclén Arana*** *el Grado Académico de Magíster en Gobierno de Tecnologías de Información, cuyo expediente debe ser remitido al Consejo de Facultad para su aprobación.*

Siendo las 21:25 *horas, el Presidente del Jurado Examinador da por concluido el acto académico de Sustentación de Tesis.*

DRA. NORA BERTHA LA SERNA PALOMINO
Presidente

MG. RÓMULO FERNANDO LOMPARTE ALVARADO
Miembro Asesor

MG. JULIO CÉSAR ROJAS MEDINA
Miembro

DRA. LUZ SUSSY BAYONA ORÉ
Miembro

MG. CIRO AGUILAR LINARES
Miembro

FICHA CATALOGRÁFICA

FACTORES QUE AFECTAN LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES PÚBLICAS PERUANAS, DE ACUERDO A LA NTP-ISO/IEC 27001

Javier Alfonso Seclén Arana
Lima - Perú, 2016
Orientador: Mg. Rómulo Lomparte Alvarado
Disertación: Magister en Gobierno de Tecnologías de Información

Universidad Nacional Mayor de San Marcos
Escuela de Posgrado
Facultad de Ingeniería de Sistemas e Informática, 2016
Unidad de Posgrado
Páginas: 255

A mis padres, motivo de mi vida y de todas mis acciones, quienes con sus expectativas hicieron que la meta sea un sueño de mucha alegría para todos.

A todas aquellas personas que de uno u otro modo me ayudaron para culminar este trabajo y que con su incansable aliento y profesionalidad constituyeron un invalorable apoyo.

Y, por encima de todo, doy gracias a Dios por conducir mi vida por un camino lleno de fe y esperanza.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE GRAFICOS

RESUMEN

La tesis titulada *"Factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas Peruanas de acuerdo a la Norma Técnica Peruana NTP-ISO/IEC 27001"* es una investigación que pretende identificar las causas que restringen la implementación del Sistema Gestión de Seguridad de la Información -SGSI- en las Entidades Públicas.

El propósito de este estudio es realizar una investigación de tipo cualitativa que permita utilizar una estrategia de recopilación de información de una manera organizada y estructurada, a través de la realización de entrevistas, para identificar las restricciones y facilidades que encuentran las entidades públicas, que permitan obtener información de apoyo a la mejora en la implementación de las políticas de seguridad de información de las entidades integrantes del Sistema Nacional de Informática.

En la presente investigación cualitativa, se han realizado 07 entrevistas a profundidad con Oficiales de Seguridad de la Información, encargados de la implementación del SGSI en sus respectivas instituciones públicas, de acuerdo a la NTP-ISO/IEC 27001.

Finalmente, se han establecido las conclusiones y recomendaciones que permitan encontrar un punto de equilibrio entre el alineamiento de TI con la estrategia de negocio de la organización y el control de riesgos de seguridad de la información, que faciliten la evaluación del nivel de complejidad de los factores que no permiten el desarrollo de la implementación total de la NTP-ISO/IEC 27001 y cómo estos terminan afectando a la gestión de los procesos de negocio de las organizaciones.

Palabras Clave. *Sistema de Gestión de Seguridad de la Información (SGSI), Norma Técnica Peruana NTP-ISO/IEC 27001, Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), Entidades Públicas Peruanas, Sistema Nacional de Informática.*

SUMMARY

The thesis entitled "Factors affecting the implementation of Management System Information Security on Public Bodies Peruvian according to Peruvian technical Norm NTP-ISO/IEC 27001" in a qualitative research that aims to identify the factors constraining the implementation of the Management System Security of Information -ISMS- in Public Administration Entities.

The purpose of the study is an investigation of qualitative type that allows using a strategy of gathering information in an organized and structured manner, through conducting interviews to identify constraints and facilities that are public entities that allow information to support the improvement in the implementation of information security policies of the entities of the National System of Information.

In this qualitative research, they have been conducted 07 in-depth interviews with Officials Information Security responsible for implementing the ISMS in their public institutions according to the NTP-ISO/IEC 27001.

Finally, we have established the conclusions and recommendations that strike a balance between the alignment of IT with the business strategy of the organization and risk control information security, to facilitate evaluation of the level of complexity of factors that prevent the development of full implementation of the NTP-ISO/IEC 27001 and how they end up affecting the management of business processes of the organizations.

Keywords. *Management System Information Security (ISMS), Peruvian Technical Norm NTP-ISO/IEC 27001, Office of E-Government and Informatics National Body (ONGEI), Peruvian Public Entities, National IT System.*

CAPITULO 1 – INTRODUCCIÓN

1.1. Situación Problemática

En la actualidad, el desarrollo de las nuevas tecnologías ha dado un giro radical a la forma de hacer negocios, a la vez que ha aumentado los riesgos para las empresas que se exponen a nuevas amenazas. Para proteger a nuestras organizaciones de todas estas amenazas es necesario conocerlas y afrontarlas de una manera adecuada.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad de la información protege a las organizaciones de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar sus daños y maximizar el retorno de las inversiones y las oportunidades de negocio. Dicha seguridad se consigue implementando un conjunto adecuado de controles, los que necesitan ser establecidos, implementados, monitoreados, revisados y mejorados

donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización.

Un Sistema de Gestión de Seguridad de la Información - **SGSI** - es un conjunto de políticas y procedimientos cuyo objetivo es administrar la Seguridad de la Información de una Organización, proporcionando una metodología sistemática, documentada y fuertemente enfocada en los riesgos que pueda enfrentar una organización.

La norma estándar internacional ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información en una organización. Dicha norma, establece los procedimientos adecuados, así como la implementación de controles de seguridad basados en la evaluación de los riesgos y en una medición de su eficacia. Se ha dispuesto que la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), adscrito a la Presidencia del Consejo de Ministros, coordine de manera permanente con las entidades públicas integrantes del Sistema Nacional de Informática respecto de la aplicación de la normatividad del SGSI vigente. (NTP-ISO/IEC 27001:2014)

El problema fundamental que da origen a este trabajo de investigación es que, al presente, a pesar de que el Gobierno Peruano ha venido impulsando todo un conjunto de normativas -referida en Antecedentes- respecto de la obligatoriedad de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en las Entidades Públicas Peruanas, aún no se ha logrado el nivel de desarrollo definido en dichas normas.

El propósito de este estudio es realizar una investigación que permita utilizar una estrategia de recopilación de información de una manera organizada y

estructurada a través de la realización de entrevistas para identificar las restricciones y facilidades que encuentran las entidades públicas, donde se establecerá un conjunto de variables de estudio que permitan su análisis y obtención de resultados que respondan al problema de investigación propuesto.

El presente trabajo de investigación tiene por finalidad analizar y evaluar todos aquellos aspectos que afectan el desarrollo del proceso de implementación del Sistema de Gestión de Seguridad de la Información en las entidades del sector público, las cuales no vienen efectivizándose respecto de la implementación final con el consecuente desarrollo del Gobierno Electrónico Peruano, a pesar de la serie de normativas gubernamentales emitidas referentes a la seguridad de la información.

1.2. Formulación del Problema de Investigación

De acuerdo con Rodríguez Peñuelas (2003), el problema de investigación es el inicio o detonador de toda indagación; es lo que desencadena el quehacer científico. El problema es una dificultad, es lo que se quiere averiguar, explicar o resolver. Por tanto, plantear el problema no es sino afinar y estructurar más formalmente la idea de investigación.

Bajo esta perspectiva, la interrogante central que orienta nuestro trabajo y que buscamos respuesta en la presente investigación es: ***¿Cuáles son los factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas Peruanas?***

Con el objeto de sistematizar nuestro trabajo, de la pregunta planteada anteriormente, se han derivado otras interrogantes, que contienen las variables más

relevantes de dicho problema y que además formaron parte de nuestros instrumentos de recolección de información.

Méndez (1999, p.67) señala que cada pregunta formulada debe de contener en su contenido variables del problema planteado, con lo cual se orienta la formulación de objetivos de investigación. Esto, menciona que se denomina sistematización del problema.

En este sentido, la sistematización del problema se formula a través de las siguientes preguntas:

1°) ¿Cuáles son los principales problemas que afectan actualmente a las entidades públicas para la implementación del SGSI en sus instituciones?

2°) ¿Cómo ha sido el proceso de implementación del SGSI en las entidades públicas?

3°) ¿Cuáles son los principales obstáculos y riesgos identificados para la implementación del SGSI según la normatividad vigente?

4°) ¿Qué beneficios han obtenido las entidades públicas al implementar el SGSI?

1.3. Justificación del Problema de Investigación

Esta investigación es llevada a cabo debido a la necesidad y obligatoriedad (R.M. N° 004-2016-PCM - Anexo 7) que tienen las entidades públicas peruanas de tener en cuenta los elementos del comportamiento organizacional dentro de una cultura organizativa para implementar una estrategia efectiva de seguridad de la información, con un enfoque de negocio, en una situación de globalización y restricciones presupuestarias, en el cual existe inquietud por conocer los diversos

factores que en los últimos años han contribuido a que no se culmine exitosamente el ciclo de implementación del SGSI.

Además, la recientemente aprobada Política Nacional de Gobierno Electrónico (D.S. N° 081-2013-PCM) tiene entre sus pilares el Objetivo Estratégico N° 3 donde dice: *"Garantizar la Integridad, Confidencialidad y Disponibilidad de la información en la Administración Pública mediante mecanismos de la Seguridad de la Información gestionada, así como articular los temas de Ciber-Seguridad del Estado"*.

Bajo este contexto, es de gran importancia que se establezcan estrategias de implementación del SGSI en la Administración Pública Peruana basadas en la Norma Técnica Peruana vigente actual, que estén más orientadas a dotar de una estructura organizacional de gestión de la información que permita el alineamiento de TI con la estrategia de negocios de las organizaciones, el logro de beneficios, la reducción de costos, el control de riesgos y en general la mejora de las operaciones de TI en las organizaciones. Ya que, si bien existe una comprensión emergente que los riesgos de TI en una organización son importantes y necesitan ser considerados, la evaluación del riesgo es aún inmadura y está en desarrollo. Además, las responsabilidades por la seguridad de la información son asignadas a un coordinador (oficial de seguridad de la información), pero sin autoridad gerencial. Finalmente, la concientización de seguridad de información está fragmentada y limitada en las organizaciones (cultura organizacional casi nula).

Los resultados de la investigación permitirán que dichas variables encontradas puedan ser utilizadas como información de apoyo a la mejora de las políticas de seguridad de información de las entidades integrantes del Sistema Nacional de Informática del Sector Público, de tal manera que les permita encontrar un punto de

equilibrio entre el alineamiento de TI con la estrategia de negocio de la organización y el control de riesgos de seguridad de la información, que faciliten la evaluación del nivel de complejidad de los factores que no permiten el desarrollo de la implementación total de la NTP-ISO/IEC 27001 y cómo estos terminan afectando a la gestión de los procesos de negocio de dicha organización (Gobierno de TI).

1.4. Objetivos de la Investigación

1.4.1. Objetivo General

El objetivo de esta investigación es analizar las principales limitaciones y problemas que vienen enfrentando las entidades del sector público en la implementación del SGSI, así como también investigar las estrategias y metodologías que vienen aplicando las entidades públicas que ya han completado su ejecución, los beneficios obtenidos de haberlo realizado en sus instituciones y la importancia de fomentar la capacitación y especialización en seguridad de la información que permitan un desarrollo integral de esta implementación en las entidades del Estado.

1.4.2. Objetivos Específicos

1.- Identificar y describir los principales problemas de implementación -previas a la implementación- que afectan a las entidades púbicas peruanas.

2.- Analizar las estrategias operacionales para impulsar entre las políticas públicas a las relacionadas con las políticas de seguridad de la información, siendo necesaria también tener estrategias de continuidad de dichos programas.

3.- Definir los obstáculos y dificultades que las entidades públicas peruanas enfrentan -durante la implementación- al efectuar la ejecución del SGSI.

4.- Identificar los beneficios obtenidos por la implementación del SGSI en las instituciones públicas que ya culminaron dicho proceso, y señalar de qué manera han sido aplicadas durante el desarrollo del mismo.

5.- Para aquellas entidades públicas que han culminado el proceso de implementación del SGSI, se plantea proponer alternativas de solución referentes a la capacitación y profesionalización de expertos en seguridad de la información que puedan conducir exitosamente planes estratégicos de implementación de SGSI en las entidades del sector público peruano.

1.5. Importancia del Estudio de Investigación

La importancia del presente estudio de investigación radica en la necesidad que tienen las organizaciones públicas peruanas de tener en cuenta los elementos del comportamiento organizacional dentro de una cultura organizativa para implementar una estrategia efectiva de seguridad de la información, con un enfoque de negocio, en una situación de globalización y restricción.

Los beneficiarios de esta investigación serán: *Primero*, la ONGEI porque tendrá mayores elementos para dirigir, implementar y supervisar la implementación de los Sistemas de Seguridad de la Información en el marco del Plan de Desarrollo de la Sociedad de la Información en el Perú; y *Segundo*, las entidades públicas que integran el Sistema Nacional de Informática porque en el futuro contarán con disposiciones generales de Estado que permitan levantar las restricciones y mejorar las facilidades que actualmente encuentren para el desarrollo de esta normatividad.

1.6. Naturaleza del Estudio de Investigación

La investigación que se pretende realizar tiene las siguientes características:

Por su estrategia técnico-metodológica, *la investigación es cualitativa* porque pretende identificar los factores que restringen la implementación del Sistema Gestión de Seguridad de la Información en las Entidades de la Administración Pública según la NTP-ISO/IEC 27001:2014.

Por su finalidad, *la investigación es básica* porque pretende desarrollar una teoría respecto de las facilidades y restricciones para la implementación de la NTP 27001 dentro de las instituciones del Estado.

Por los objetivos, *la investigación es descriptiva* porque pretende identificar todos aquellos aspectos que afectan el desarrollo del proceso de implementación del Sistema Gestión de Seguridad de la Información en las Entidades Públicas.

Por los tipos de datos que se trabajarán, *éstos serán Primarios* porque para identificar los factores que restringen la implementación del Sistema Gestión de Seguridad de la Información se realizaron entrevistas que permitirán levantar información de primera mano.

Por el grado de control, *la investigación es no experimental* porque no podríamos controlar todas las variables identificadas.

Por la secuencia temporal, *la investigación es transversal* porque no se realizará el método de investigación en distintos momentos para ver su evolución, sino que se realizará en un solo periodo de tiempo.

1.7. Pregunta del Estudio de Investigación

La pregunta de investigación para el presente proyecto es la siguiente:

¿Qué factores son los que afectan la implementación del Sistema Gestión de Seguridad de la Información en las Entidades de la Administración Pública según la NTP-ISO/IEC 27001?

Las conclusiones que esta investigación pretende obtener podrían ser utilizadas como información de apoyo a la mejora de las políticas de seguridad de información de las entidades integrantes del Sistema Nacional de Informática del Sector Público, de tal manera que les permita encontrar un punto de equilibrio entre el alineamiento de TI con la estrategia de negocio de la organización y el control de riesgos de seguridad de la información, que faciliten la evaluación del nivel de complejidad de los factores que no permiten el desarrollo continuo y progresivo de la implementación total de la NTP-ISO/IEC 27001 y cómo estos terminan afectando a la gestión de los procesos de negocio de dicha organización (Gobierno de TI).

1.8. Supuestos

En el presente estudio se asume que la Oficina Nacional de Gobierno Electrónico e Informática -ONGEI- continuará liderando el Proyecto de Gobierno Electrónico en el Perú, y que cada vez más tendrá un rol protagónico como ente articulador y promotor de la implementación de la Norma Técnica Peruana NTP-ISO/IEC 27001. Así como también, no cambiará el apoyo político respecto del programa de modernización del Estado ni la Agenda Digital Peruana 2.0.

1.9. Limitaciones

El presente estudio de investigación abarcará a los Organismos Públicos que están obligados a implementar la NTP-ISO/IEC 27001, y que son parte integrante de las entidades del Sistema Nacional de Informática del Perú, dentro del cual está inmersa la muestra elegida.

La unidad de análisis está limitada a los Directores de Informática u Oficiales de Seguridad de la Información que participan en la implementación de la norma.

1.10. Resumen

En el presente capítulo, se ha descrito la situación problemática encontrada, lo que me lleva a realizar una investigación que permita determinar qué factores son los que dificultan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas del Sistema Nacional de Informática del Estado Peruano. Además se ha definido la situación problemática, el propósito del estudio de investigación, los objetivos a desarrollar en la investigación, la importancia del problema, las limitaciones, los supuestos y la pregunta de investigación para el proyecto de investigación.

CAPÍTULO 2 – MARCO TEÓRICO

La seguridad de la información es importante en organizaciones, tanto del sector público como del privado, y para proteger las infraestructuras críticas. La interconexión de las redes públicas y privadas y la compartición de los recursos de información, aumentan la dificultad de lograr el control de los accesos.

Se requiere por tanto que, para gestionar eficientemente la seguridad de la información, todos los miembros de la Organización tomen conciencia de su importancia y el papel que juegan en generar aportes de calidad y eficacia en los servicios críticos de la Entidad. Por otro lado, la cultura organizacional dificulta la implantación de una estrategia de protección de la seguridad de la información. Se ha comprobado que existe una relación directa entre la efectividad del establecimiento de una estrategia de la seguridad de la información y la cultura organizacional de una Organización. **[45].**

Bajo este contexto, se ha encontrado que existe un amplio panorama de normas técnicas, estándares y mejores prácticas que han sido emitidas por las entidades gubernamentales, institutos de normalización, organizaciones independientes y la comunidad académica, desde las cuales se ha elaborado una relación documentada, que refleja el estado del arte en lo referente a los Sistemas de Gestión de Seguridad de la Información - SGSI.

Es necesario agregar además que el presente estudio de investigación se realizará tomando como referencia los diferentes estudios realizados en Seguridad de la Información en el Perú, tales como: La VIII Encuesta Nacional de Recursos Informáticos de la Administración Pública (ENRIAP, 2010), II Encuesta Nacional de Seguridad de Información, Informe de Fraude en el Perú 2011 (KPMG), IV Encuesta Latinoamericana de Seguridad de la Información 2012 (ACIS-ISACA), Informe: 10 grandes errores de Seguridad de Información en el Perú 2008 (JackSecurity), Informe: Gobierno de Seguridad de la Información - Nivel de Maduración Perú 2008 (JackSecurity), entre otros.

2.1. Evolución histórica de la Seguridad de la Información

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Su origen se remonta desde 1901, y como primera entidad de normalización a nivel mundial, la organización británica BSI (British Standards Institution) es responsable de la publicación de importantes normas como:

- 1979: Publicación BS 5750 - ahora ISO 9001
- 1992: Publicación BS 7750 - ahora ISO 14001
- 1996: Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con el objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información. La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación.

Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como el estándar ISO 27001, al tiempo que se revisó y actualizó la ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión. En el 2013, se revisa y actualiza la ISO 27001 y se publica como ISO 27001:2013.

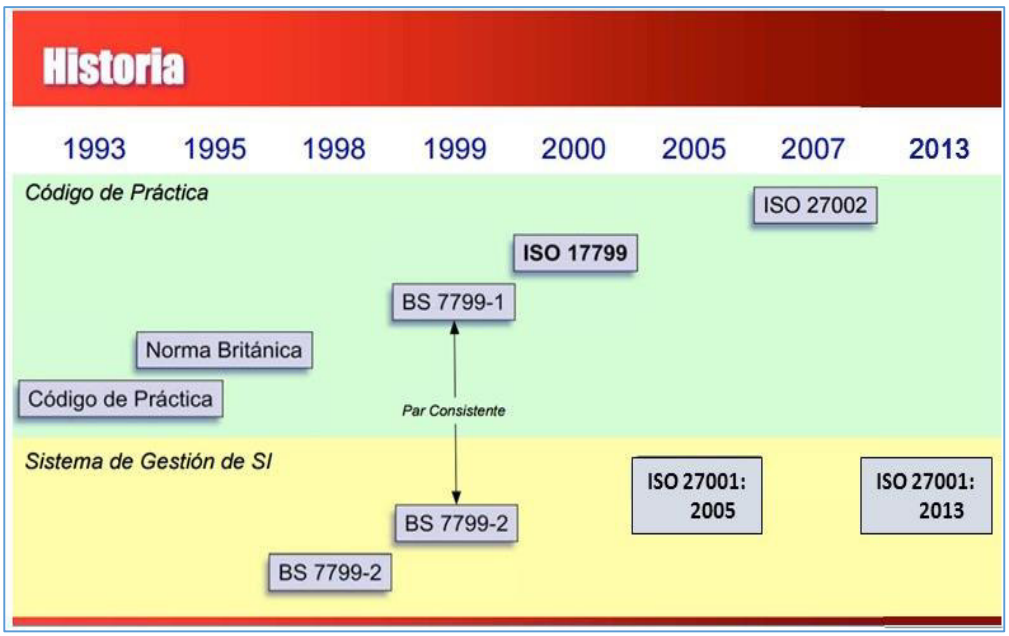


Gráfico N° 1: **Evolución de los estándares de la Seguridad de la Información**
Fuente: **Estándar de Seguridad de Información (GPC Global)**
http://www.gcpglobal.com/docs/Intro_ISO27001.pdf

La familia ISO/IEC 27000 es un conjunto de estándares desarrollados por la ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Al respecto, tenemos la familia de normas de la serie ISO/IEC 27000, que agrupa una serie de normas y estándares -que incluyen una serie de normativas sobre gestión de riesgos, métricas, auditorías y guías de implementación, etc.- las mismas que están alineadas con los requerimientos especificados en la norma 27001. **[24] [39] [40] [41]**

En la línea de los ISO 27000, existe una amplia variedad de estos tales como las siguientes:

- **ISO 27001:** Requisitos para establecer un SGSI;
- **ISO 27002:** Guía de Buenas Prácticas en objetivos de control y controles recomendados de Seguridad de la Información;
- **ISO 27003:** Guía de implementación de SGSI junto a información de uso del Esquema PDCA (Plan-Do-Check-Act);
- **ISO 27004:** Especificación de métricas para determinar la eficiencia del SGSI;
- **ISO 27005:** Guía de técnicas de Gestión de Riesgos;
- **ISO 27006:** Especificación de requisitos para acreditación de entidades de auditoría y certificación del SGSI;
- **ISO 27011:** Guía de auditoría del SGSI;
- **ISO 27031:** Guía de continuidad de negocios en cuanto a TIC;
- **ISO 27032:** Guía de Cyber-Seguridad;
- **ISO 27033:** Guía de Seguridad de Redes;
- **ISO 27034:** Guía de Seguridad de Aplicaciones.

2.2. Estándares y Regulaciones de la Seguridad de la Información

En el nuevo contexto en el que operan las organizaciones, las tecnologías de la información juegan un papel fundamental al acortar y automatizar los ciclos de negocio y convertirse en pieza angular de los procesos de una compañía. En este mercado en constante aceleración, las empresas requieren actuar con mayor agilidad, flexibilidad y mejores niveles de servicio.

Pero al mismo tiempo, las organizaciones se enfrentan a la proliferación de regulaciones, amenazas, riesgos, dispositivos, usuarios, procesos y datos. Un reto que pone en jaque al área de TI, por lo que las organizaciones tienen una doble

responsabilidad respecto a la información. Por un lado, proteger el dato que se ha convertido un activo de valor y, por otro, cumplir con las regulaciones aplicables al sector correspondiente.

Una de las principales necesidades que tienen las organizaciones actualmente es la gestión de la seguridad de los Sistemas de Información, entendiendo que en este contexto los sistemas de información no están limitados al ámbito tecnológico.

Para atender estas necesidades, muchas organizaciones a nivel mundial (ISO, BSI, NIST, IEEE, ITGI, etc.) han desarrollado y continúan desarrollando estándares, mejores prácticas, metodologías y herramientas que facilitan una gestión eficiente de la seguridad de la información.

A continuación, se hace un alcance de las principales regulaciones existentes respecto de la seguridad de la información:

2.2.1. NIST: El Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology), es un organismo federal no regulador que forma parte de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión del NIST consiste en elaborar y promover patrones de medición, normas y tecnología con el fin de realzar la productividad, facilitar el comercio y mejorar la calidad de vida.

Entre sus informes publicados destaca el **NIST 800-100. "Information Security Handbook: A Guide for Managers"**, Guía de 176 páginas que analiza el buen gobierno de la seguridad de la información, el desarrollo de sistemas, la formación y la concienciación en seguridad, el control de riesgos, las inversiones en tecnología, las telecomunicaciones y su interconexión, el rendimiento del SGSI, la planificación de la seguridad, los planes de contingencias, la certificación y auditoria de la

seguridad, la contratación de servicios y productos de seguridad, la respuesta ante incidentes, la gestión de configuraciones. Una guía útil para tener una visión global de la Seguridad de la Información dentro de las Organizaciones.

2.2.2. BSI: El Instituto de Normas Británico (British Standards Institution) publicó en 2006 la tercera parte de BS 7799, dedicada a la gestión de riesgos de seguridad de la información.

BSI es una multinacional cuyo fin se basa en la creación de normas para la estandarización de procesos. Es un organismo colaborador de ISO y proveedor de estas normas, son destacables la ISO 9001, ISO 14001 e ISO 27001. Entre sus actividades principales se incluyen la certificación, auditoría y formación en las normas.

2.2.3. ISO 27001: (evolucionada a partir de BS 7799-2) indica que las organizaciones deben identificar, evaluar, tratar y gestionar los riesgos de seguridad de la información, pero no da indicaciones más detalladas de cómo realizar dicho proceso ni de cómo situar dichos riesgos en el marco de los riesgos generales de la empresa.

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

2.2.4. COBIT: Objetivos de Control para la Información y Tecnologías relacionadas (Control OBjectives for Information and related Technology) es un

conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoria y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores." Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.

***2.2.5. ITIL*:** La Biblioteca de Infraestructura de Tecnologías de Información (Information Technology Infrastructure Library), es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía para que abarque toda infraestructura, desarrollo y operaciones de TI.

***2.2.6. HIPPA*:** La Ley de responsabilidad y transferibilidad de los seguros médicos (Health Insurance Portability & Accountability Act) de 1996, ley pública 104-191, que modifica el código del Internal Revenue Service de 1986. También conocida como la Ley de Kennedy-Kassebaum.

El Título II incluye una sección, Simplificación administrativa, que exige:

1. Mayor eficiencia en la asistencia médica por medio de la estandarización del intercambio electrónico de datos, y
2. La protección de la confidencialidad y seguridad de los datos médicos, a través del establecimiento y cumplimiento de estándares.

Más específicamente, la HIPAA pide:

1. La estandarización de los datos electrónicos administrativos, financieros y de salud de los pacientes
2. Identificadores médicos únicos para personas, empleados, planes de salud y proveedores de cuidados médicos
3. Normas de seguridad que protejan la confidencialidad y la integridad de la "información médica identificable a nivel personal" pasada, presente o futura.

En resumen: cambios radicales en la mayoría de los sistemas de información administrativos de transacciones médicas.

***2.2.7. CIPA*:** La Ley de Protección de Niños en Internet (Children's Internet Protection Act), es una ley federal promulgada por el Congreso Estadounidense para manejar asuntos relacionados con el acceso a contenido ofensivo en Internet, en las computadoras de las escuelas y bibliotecas. La CIPA establece ciertos tipos de requisitos para cualquier escuela o biblioteca que reciba apoyo financiero destinado a cubrir su acceso a Internet o a conexiones internas del programa “E-rate,” un

programa que da acceso a ciertas tecnologías de comunicaciones a precios moderados, para las escuelas y bibliotecas elegibles. A principios de 2001, la Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) emitió normas de implementación de la CIPA.

***2.2.8. SARBANES OXLEY*:** La Ley Sarbanes Oxley, cuyo título oficial en inglés es Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (30 de julio de 2002), es una Ley de Estados Unidos también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. También es llamada SOx, SarbOx o SOA.

La Ley Sarbanes Oxley nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

Esta ley, más allá del ámbito nacional, afecta a todas las empresas que cotizan en NYSE (Bolsa de Valores de Nueva York), así como a sus filiales.

***2.2.9. GRAMM-LEACH-BLILEY ACT (GLBA) Servicios Financieros*:** Las instituciones gobernadas por la GLBA:

- ✓ Deberán garantizar la seguridad y confidencialidad de los registros e información de clientes.
- ✓ Deberán estar protegidas contra amenazas anticipadas o riesgos de seguridad o integridad de registros
- ✓ Deberán estar protegidos en contra de accesos no autorizados hacia o el uso de registros o información que pudiera resultar en el daño sustancial o inconveniencia hacia cualquier cliente.

2.3. Antecedentes del problema de investigación

La Oficina Nacional de Gobierno Electrónico e Informática - ONGEI - de la Presidencia del Consejo de Ministros, como ente rector de la implementación de la Política Nacional de Gobierno Electrónico, desde su creación, ha emitido normas en forma orgánica y sistematizada, con el fin de desarrollar la Seguridad de la Información de acuerdo a estándares internacionales.

A continuación, haremos una revisión integral respecto de los antecedentes de la seguridad de la información, lo cual nos dará un mayor panorama del problema de investigación:

a) **1994 - Resolución Jefatural 362-94-INEI**
   Aprueba la Directiva 016-94-INEI/SJI "Normas para la prevención, detección y eliminación de Virus Informático en los equipos de cómputo de la administración pública"

b) **1995 – Resolución Jefatural 076-95-INEI**
   Aprueba la Directiva 007-95-INEI/SJI "Recomendaciones Técnicas para la Seguridad e Integridad de la Información que se procesa en la Administración Pública"

c) **1995 - Resolución Jefatural 090-95-INEI**
   Aprobar la Directiva 008-95-INEI/SJI "Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública".

d) **2001 – Resolución Jefatural 347-2001-INEI**
   Aprueban Directiva "Normas y Procedimientos Técnicos para garantizar la Seguridad de la Información publicadas por las entidades de la Administración Pública".

e) 2002 – Resolución Jefatural 386-2002-INEI

Normas técnicas para el almacenamiento y respaldo de la información procesada por las entidades de la administración pública.

f) 2004 – Resolución Ministerial 224-2004-PCM

Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004.EDI. Tecnología de la Información: Código de Buenas Prácticas para la gestión de la Seguridad de la Información. Primera Edición" en las entidades del Sistema Nacional de Informática.

En esta normativa, se establecieron los lineamientos de buenas prácticas para la correcta gestión de seguridad de la información y se fijó un plazo de 18 meses para su implementación en todas las entidades del Estado. Luego, en el año 2005, se ampliaría el plazo de cumplimiento hasta al 30 de junio de 2006.

g) 2004 – Resolución Ministerial 310-2004-PCM

Autorizan Ejecución de la "Primera Encuesta de Seguridad de la Información en la Administración Pública – 2004".

h) 2005 – Resolución Ministerial 395-2005-PCM

Modifican plazos para implementar la Norma Técnica Peruana cuyo uso obligatorio se aprobó mediante las Resolución Ministerial 224-2004-PCM. El plazo de cumplimiento se amplía al 30 de junio del 2006.

i) 2007 – Resolución Ministerial 246-2007-PCM

Se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

En esta norma se recomienda que las entidades consideren las actividades necesarias en sus respectivos Planes Operativos Informáticos (POI) para su implementación.

j) 2007 – Resolución 1-2007/INDECOPI-CRT

NTP ISO/IEC 17799:2007 - Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. 2da. edición. Esta Norma Técnica Peruana establece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad, así como proporcionar confianza en las relaciones entre organizaciones.

k) 2008 – Resolución de Contraloría 352-2008-CG

Aprobar la política de seguridad de la información para la Contraloría General de la República.

l) 2009 – Resolución Ministerial 360-2009-PCM

Crean el Grupo de Trabajo denominado Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (**PeCERT**).

PeCERT es el ente encargado de liderar los esfuerzos para proveer a la nación de una postura segura en el ámbito de la seguridad informática y cuyo objetivo es brindar apoyo para elevar los niveles de seguridad de la información en el sector público coordinando entre las entidades de la Administración Pública Nacional para la prevención, detección, manejo y recopilación de información y

desarrollo de soluciones para incidentes de seguridad y servir como repositorio de la información referente a eventos o hechos en los cuales esté involucrada la seguridad en las redes, mediante la investigación, desarrollo, actualización de la información y difusión.

m) 2009 – Resolución 29-2009/INDECOPI-CNB

NTP ISO/IEC 27005:2009 - Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información (Establece lineamientos para la gestión del riesgo en seguridad de la información.

Esta Norma Técnica Peruana apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñado para asistir a la implementación satisfactoria de la seguridad de la información en base a un enfoque de gestión del riesgo. Es importante conocer los conceptos, modelos, procesos y tecnologías descritos en las normas ISO/IEC 27001 e ISO/IEC 27002 para entender cabalmente esta NTP.

Esta Norma Técnica Peruana es aplicable a todo tipo de organizaciones (por ejemplo: empresas comerciales, dependencias gubernamentales, organizaciones sin fines de lucro) que tratan de administrar los riesgos que podrían comprometer la seguridad de la información de la organización).

NTP ISO/IEC 27006:2009 - Tecnología de la información. Técnicas de seguridad. Requisitos para los organismos que realizan auditorías y certificaciones de los sistemas de gestión de la seguridad de la información. (ISO/IEC 27006:2007 EDI. Information Technology - Security Techniques - Requirements for bodies providing audit and certification of information security management systems)

n) 2010 - Resolución Ministerial N° 187-2010-PCM

Autorizan Ejecución de la "Segunda Encuesta de Seguridad de la Información en la Administración Pública – 2010".

o) 2010 – Resolución 060-2010/SUNARP/SN

Aprobar el Reglamento de Seguridad de la Información de la Superintendencia Nacional de los Registros Públicos – SUNARP.

p) 2010 – Resolución 26-2010/CNB-INDECOPI

NTP ISO/IEC 28001:2010 - DI. Sistema de gestión de la seguridad. Requisitos para los organismos que realizan auditorías y certificaciones de los sistemas de gestión de la seguridad de la información para la cadena de suministro.

Buenas prácticas para la implantación de la seguridad para la cadena de suministros, evaluación de planes y requisitos y guía. Proporciona los requisitos y sirve de guía a las organizaciones en las cadenas de suministro internacionales para:

- Desarrollar e implementar procesos de seguridad en la cadena de suministro;
- Establecer y documentar un nivel mínimo de seguridad en la cadena o cadenas de suministro o en una parte de una cadena de suministro;
- Asistir en el cumplimiento del criterio del Operador Económico Autorizado (OEA) aplicable, establecido en el Marco de la Organización de Aduanas y en la conformidad con los programas nacionales de seguridad en la cadena de suministro.

q) 2011 – Resolución Ministerial 197-2011-PCM

Establecen fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información". Esta Norma Técnica Peruana pone como fecha límite del mismo el 31 de diciembre del 2012, siendo de aplicación obligatoria para 50 entidades de la Administración Pública.

r) 2012 – Resolución Ministerial 129-2012-PCM

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

Esta Norma Técnica Peruana, establece la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) - de manera obligatoria y progresiva según un cronograma incremental en un plazo máximo de 27 meses - en 71 entidades integrantes del Sistema Nacional de Informática del sector público, con la finalidad de coadyuvar en el desarrollo y fortalecimiento de la infraestructura de Gobierno Electrónico en el Perú. Siendo está norma la que actualmente está vigente.

s) 2012 – Resolución 84-2012/CNB-INDECOPI

NTP ISO/IEC 27003:2012 - Técnicas de seguridad. Directrices para la implementación de un sistema de gestión de la seguridad de la información. 1a. ed. (ISO/IEC Information technology -- Security techniques -- Information security management system implementation guidance)

NTP ISO/IEC 27004:2012 - Técnicas de seguridad. Gestión de la seguridad de la información. Medición. 1ra. edición. Provee guías para el desarrollo y uso de medidas y mediciones, con el objetivo de evaluar la efectividad de un sistema de gestión de seguridad de la información (SGSI) implantado y los controles o grupo de controles tal como se especifica en ISO/IEC 27001. Esta Norma Técnica Peruana es aplicable a todo tipo y tamaño de organización.

NTP ISO/IEC 27031:2012 - Técnicas de seguridad. Directrices para la adecuación de las tecnologías de la información y las comunicaciones para la continuidad del negocio. 1ra. edición.

Describe los conceptos y principios de la preparación de las tecnologías de la información y las comunicaciones (TIC) para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos (tales como los criterios de desempeño, diseño e implantación) para la mejora de la preparación de las TIC de una organización para garantizar la continuidad del negocio. Se aplica a cualquier organización (privadas, gubernamentales y no gubernamentales, independientemente de su tamaño) desarrollando su programa de adecuación de las TIC para la continuidad del negocio (ATCN, por sus siglas en inglés), y exigiendo que sus servicios e infraestructura TIC estén listos para apoyar las operaciones de negocios en el caso de nuevos eventos e incidentes, y las interrupciones relacionadas que puedan afectar la continuidad (incluida la seguridad de la información) de las funciones críticas del negocio. También permite a una organización medir los parámetros de desempeño correlacionados con su ATCN de una manera consistente y reconocida. El objeto de esta Norma Técnica Peruana abarca todos los eventos e incidentes (incluidos los relacionados con la seguridad de la

información) que podrían tener un impacto en la infraestructura y en los sistemas TIC. Incluye y extiende las prácticas de manejo y gestión de incidentes de seguridad de la información y la planificación de la preparación de las TIC y sus servicios).

t) 2012 - Resolución 28-2012/CNB-INDECOPI

NTP ISO 27799:2010 - Informática sanitaria. Gestión de la seguridad de la información en sanidad utilizando la ISO/IEC 27002 (Esta norma define directrices para dar soporte a la interpretación e implementación en informática sanitaria de la Norma ISO/IEC 27002 y es un manual de dicha norma).

u) 2012 - Resolución Secretarial 099-2012-SGEN/RENIEC

Directiva DI-328-GI/022 - "Seguridad Informática de la red de RENIEC" (primera versión)

v) 2013 – Resolución 44-2013/CNB-INDECOPI

NTP ISO/IEC 27001:2008 (Revisada el 2013) - Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 1ra. edición. Cubre todo los tipos de organizaciones (como por ejemplo: empresas comerciales, agencias de gobierno y organizaciones sin fines de lucro). Esta NTP especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un ISMS documentado dentro del contexto de los riesgos de negocio de la organización. Especifica los requisitos para implementar los controles de seguridad adaptada a las necesidades individuales de las organizaciones o partes de las mismas.

w) 2013 – Resolución 45-2013/CNB-INDECOPI

NTP ISO/IEC 27007:2013 - Técnicas de seguridad. Lineamientos para la auditoría de sistemas de gestión de seguridad de la información. 1ra. edición. Proporciona guías sobre cómo manejar un programa de auditoría del Sistema de Gestión de Seguridad de la Información (SGSI), sobre conducir las auditorías y sobre la competencia de los auditores del SGSI, además de la guía contenida en la norma ISO 19011.

NTP ISO/IEC 27035:2013 - Técnicas de seguridad. Gestión de incidentes de seguridad de la información. 1a. ed. Proporciona guía sobre la gestión de incidentes de seguridad de la información para organizaciones grandes y medianas. Las organizaciones más pequeñas pueden usar un conjunto básico de documentos, procesos y rutinas descritos en esta NTP, dependiendo de su tamaño y del tipo de negocio relacionado a la situación de riesgo de seguridad de la información. También proporciona guía para que las organizaciones externas provean servicios de gestión de incidentes de seguridad de la información.

x) 2013 – Resolución 77-2013/CNB-INDECOPI

NTP RT ISO/IEC-TR 27008:2013 - Técnicas de Seguridad. Lineamientos para auditores sobre controles de seguridad de la información. 1ra. edición.

y) 2016 – Resolución Ministerial 004-2016-PCM

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática del Estado Peruano.

Esta NTP provee un modelo para implementar los principios en las pautas que gobiernan la evaluación del riesgo, el diseño e implementación de la seguridad, la gestión de seguridad y la reevaluación de la información en una institución. De acuerdo a esta resolución, se especifica que la implementación deberá realizarse en un plazo máximo de dos (02) años a partir de su publicación.

Estas acciones no son los únicos esfuerzos que el Gobierno Peruano ha evidenciado sobre la viabilidad de desarrollo de la seguridad de la información. A través del "***Plan de Desarrollo de la Sociedad de la Información en el Perú - la Agenda Digital Peruana 2.0***", aprobada mediante Decreto Supremo N° 066-2011-PCM, se plantean ocho (8) objetivos con sus respectivas estrategias, en el cual el Objetivo N° 7 refiere la de "Promover una administración pública de calidad orientada a la población", teniendo como Estrategia 4 la de "Implementar mecanismos para mejorar la Seguridad de la Información", así como la necesidad de contar con una estrategia nacional de ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como la disuasión del crimen cibernético que se producen mediante el uso de redes teleinformáticas, entre otros. (ONGEI, 2013 p.45)

Concordantemente, la Política Nacional de Gobierno Electrónico, aprobada mediante Decreto Supremo N° 081-2013-PCM, tiene entre sus pilares en el Objetivo N° 3: ***"Garantizar la integridad, confidencialidad y disponibilidad de la información en la Administración Pública mediante mecanismos de Seguridad de la Información gestionada, así como articular los mecanismos de ciber-seguridad del Estado"***.

Esta Política Nacional contribuye, a través del uso de las tecnologías de información, al desarrollo del país con el incremento de la competitividad, el acercamiento del Estado a los ciudadanos, la promoción de la participación ciudadana, la transparencia y el acceso a la información pública y la seguridad de la información. Asimismo, el Gobierno Electrónico en el Perú establece una serie de lineamientos estratégicos donde se ha establecido a la Seguridad de la Información como uno de estos, y donde dice: El paradigma de ***"todo a disposición de todos"*** debe manejarse de la manera más cuidadosa, velando por la integridad, seguridad y disponibilidad de los datos. Para ello, deben establecerse lineamientos en Seguridad de la Información a fin de mitigar el riesgo de expedición de información sensible del ciudadano".

Así también, en el año 2013, se aprueba la Ley N° 29733, Ley de Protección de Datos Personales (LPDP) y su reglamento, aprobado mediante Decreto Supremo N° 003-2013-JUS. La legislación sobre Protección de Datos marca una serie de límites a la utilización de los datos personales. Esto afecta a todas las empresas de nuestro país ya que, en mayor o menor medida, todas tratan o manejan datos de carácter personal de personas físicas (clientes, proveedores, empleados, colaboradores, accionistas).

Todas las empresas (públicas o privadas) deben adaptarse a la legislación teniendo en cuenta que deben conjugar, por un lado, los derechos que poseen los ciudadanos sobre el uso, tratamiento y destino de sus datos y, por otro, las medidas de tipo organizativas y técnicas que debemos establecer en nuestra organización para garantizar la seguridad de la información.

Finalmente, la Seguridad de la Información de Documentos Electrónicos se encuentra en el Decreto Legislativo N° 681 y el Decreto Legislativo N° 827, normas que establecen el uso de Microformas y la Micrograbación de documentos en formato electrónico con pleno valor legal.

Por todo lo expuesto, se pone de manifiesto la relevancia que tiene la presente investigación pues nos ha permitido obtener un marco referencial para la identificación del problema existente respecto de los factores que afectan el desarrollo continuo del proceso de implementación del Sistema de Gestión de Seguridad de la Información en las Entidades del Sector Público.

2.3.1. Estructura de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014

La Norma Técnica Peruana de Seguridad de la Información NTP-ISO/IEC 27001:2014 proporciona los requisitos necesarios para establecer, implementar mantener y mejorar continuamente un sistemas de gestión de seguridad de la información.

Este sistema de gestión preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos, y proporciona confianza a las partes interesadas en el sentido en que los riegos se manejan adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de y esté integrado con los procesos de la organización y la estructura de la gestión general. Se espera, además, que dicha implementación crezca en concordancia con las necesidades de la organización.

La Norma Técnica Peruana de Seguridad de la Información NTP-ISO/IEC 27001:2014 ha sido elaborada utilizando como antecedente al estándar internacional ISO/IEC 27001:2013, en donde no sólo se establecen cambios en el contenido sino también en la estructura respecto de la versión anterior (NTP-ISO/IEC 27001:2008).

Las principales modificaciones se ven reflejadas en la estructura y el contenido de los controles, donde el número total de dominios era de 11 y ahora son 14 y se reduce el número de controles de 133 a 113, todo como resultado de un proceso de fusión, exclusión e incorporación de nuevos controles de seguridad.

Además, en esta nueva versión de la 27001, se ha ampliado el tema del tratamiento de riesgos alineándolo con la ISO 31000 referida a la Gestión de Riesgos en forma genérica; es decir, a los riesgos de todo tipo (no sólo de seguridad de la información) que pueden afectar una organización.

De cualquier manera, el alineamiento con la ISO 31000 no significa que la ISO 27005 de Riesgos de Seguridad de la Información pierda relevancia, ya que su uso se puede justificar puesto que esta norma (27005) trata especialmente los riesgos técnicos de TI, mientras que la ISO 31000 provee un marco de trabajo más adecuado para los riesgos de negocio.

Algo muy importante de destacar es que la ISO/IEC 27001:2013 ha sido desarrollado **con base en el Anexo SL** del *"Suplemento Consolidado de las Directivas ISO/IEC",* en el cual se alinean bajo una misma estructura todos los documentos relacionados con los sistemas de gestión y evitando así problemas de integración con otros marcos de referencia.

Así pues, la nueva estructura queda como sigue:

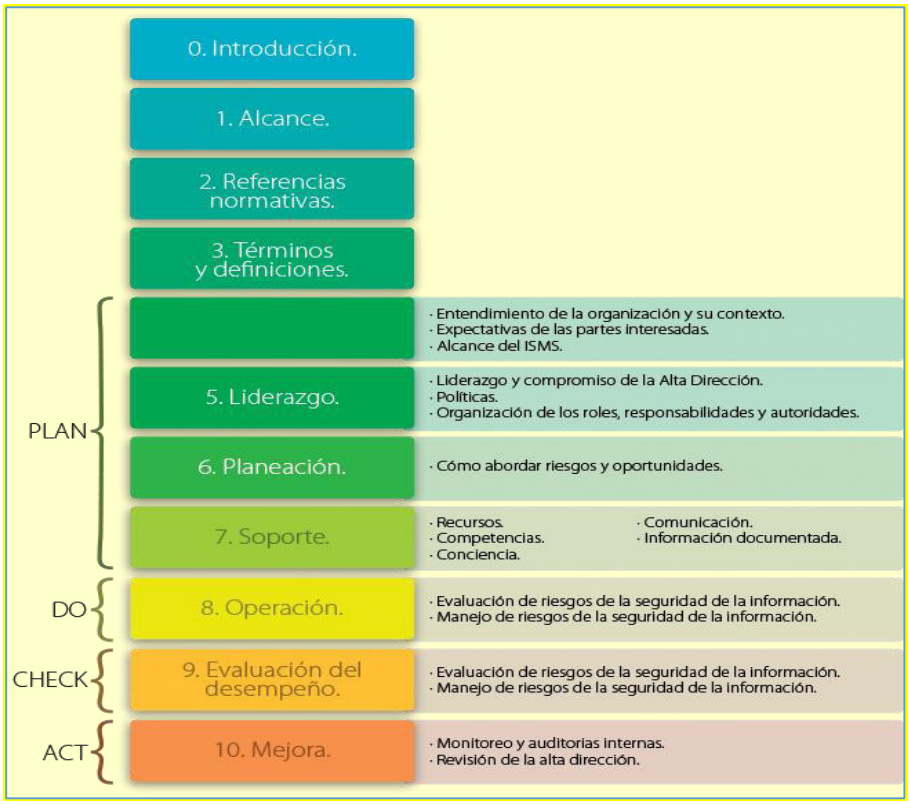


Gráfico 2: **Estructura del estándar ISO/IEC 27001:2013**

La importancia del Anexo SL radica en que todas las futuras normas de sistemas de gestión tendrán la misma estructura de referencia, de tal manera que las organizaciones que dispongan de más de una norma de sistemas de gestión no estén aisladas unas de otras con diferentes estructuras, requisitos y terminologías. Este anexo proporciona un marco para un sistema de gestión genérico y la estructura para todas las normas de sistemas de gestión nuevas y revisadas de ahora en adelante, garantizando coherencia y compatibilidad.

La metodología de implementación de la NTP-ISO/IEC 27001:2014 establece el cumplimiento de 07 fases (clausulas 04 a 10 de la norma), las cuales permitirán fomentar la alineación estratégica entre la seguridad de la información y el plan estratégico institucional, lo que tendrá como consecuencia permitir a la organización

evaluar, controlar, dirigir y comunicar de forma eficiente las actividades que están relacionadas con la información.

Respecto de los Anexos (que formaban parte de la NTP anterior), el Anexo A: "Referencia de Objetivos y Controles" continúa formando parte de este estándar, aunque según se refirió anteriormente, el número de dominios del anexo aumentó de 11 a 14. Esto debido a que algunos controles se incluían de forma superficial en ciertas áreas donde no encajaban perfectamente, y donde ahora se organiza mejor. Por otro lado, los Anexos "B" y "C", en esta nueva norma, se han eliminado.

Las fases de implementación de la NTP-ISO/IEC 27001:2014, pueden ser visualizadas en el siguiente diagrama:

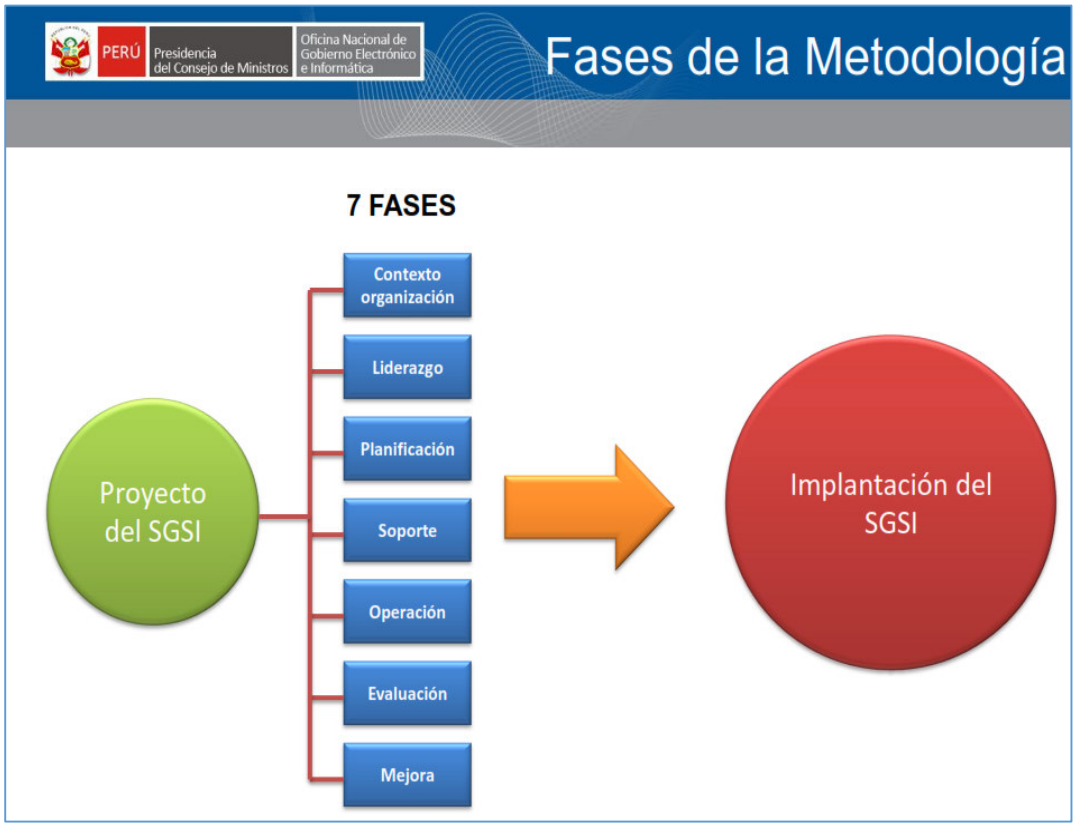


Tabla 1: **Fases de la metodología de implementación de la NTP-ISO/IEC 27001:2014**
Fuente: **ONGEI**

2.4. Estado del Arte de la Seguridad de la Información

2.4.1. Análisis de la Seguridad de la Información en el Gobierno de TI

Se entiende por Gobierno de TI al conjunto de acciones que realiza el área de TI, en coordinación con la alta dirección, para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio; constituye una parte esencial del gobierno de la empresa en su conjunto y aglutina la estructura organizativa y directiva necesaria para asegurar que TI soporte y facilite el desarrollo de los objetivos estratégicos definidos.

El Gobierno de TI es extendible a todos los servicios de TI, en especial a aquellos que considera la seguridad de la información, sustentada en las herramientas de seguridad de TI, y en el aseguramiento tanto de los activos como de los flujos de información de la empresa. Es por eso que el Sistema de Gestión de la Seguridad de la Información (SGSI) surge como un concepto relevante en las organizaciones, bajo el entendido que estas son conscientes de la relevancia de este activo corporativo, especialmente cuando en ella se fundamenta la toma de decisiones, entre ellas las de TI. **[20]**

La norma que proporciona un Marco de Gobierno de TI es la ISO 38500 que proporciona un marco de principios para que la dirección de las organizaciones evalúen, dirijan y monitoricen el uso de TI **[10].**

El Gobierno Corporativo de TI es el sistema por el cual se dirige y supervisa el estado actual y futuro del uso de TI (ISO/IEC 38500). El gobierno de TI trata principalmente con los planes para utilizar TI (en ambos contextos; estratégico y operacional), las iniciativas que crean sus usos futuros y, las actividades operacionales que constituyen su utilización actual.

El modelo de gobierno de TI presentado en ISO/IEC 38500 posiciona tres tareas claves de gobierno – evaluar, dirigir, controlar, como la clave para dar dirección hacia y, controlar el desempeñó de los roles de gestión en la conducción de la organización para la planificación, implementación y utilización operacional de TI.

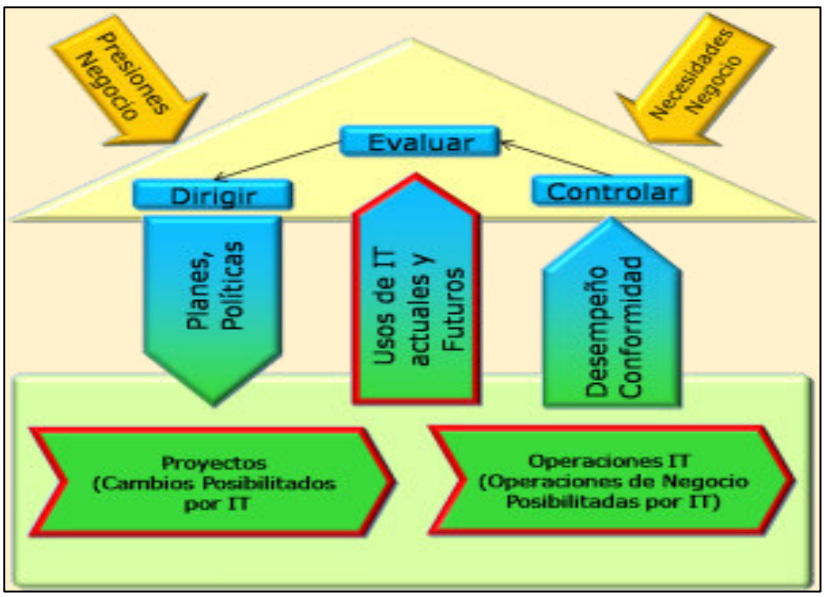


Gráfico N° 3: **Modelo de Gobierno de TI. Fuente: ISO/IEC 38500**

Esta norma define seis principios de un buen gobierno corporativo de TI:

a) Responsabilidad

Todo el mundo debe comprender y aceptar sus responsabilidades en la oferta o demanda de TI. La responsabilidad sobre una acción lleva aparejada la autoridad para su realización.

b) Estrategia

La estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las TI. Los planes estratégicos de TI satisfacen las necesidades actuales y previstas derivadas de la estrategia de negocio.

c) Adquisición

Las adquisiciones de TI se hacen por razones válidas, basándose en un análisis apropiado y continuo, con decisiones claras y transparentes.

Hay un equilibrio adecuado entre beneficios, oportunidades, costes y riesgos tanto a corto como a largo plazo.

d) Rendimiento

La TI está dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras.

e) Conformidad

La función de TI cumple todas las legislaciones y normas aplicables. Las políticas y prácticas al respecto están claramente definidas, implementadas y exigidas.

f) Conducta humana

Las políticas de TI, prácticas y decisiones demuestran respecto por la conducta humana, incluyendo las necesidades actuales y emergentes de toda la gente involucrada.

Por tanto, el Gobierno de TI cumple un rol fundamental en la Organización toda vez que asegura mejoras eficientes y eficaces en los procesos de la empresa, relacionados entre sí.

Esta gobernanza debe estar configurada de tal manera que en el menor tiempo posible brinde directrices que orienten a la alta gerencia en los mecanismos para aplicar procedimientos de gobierno, como parte integral de los procesos, en procura del logro de los objetivos organizacionales.

Actualmente, las empresas se tienen que dotar de una estructura de gestión de la información que permita: el alineamiento de TI con la estrategia de negocio, el logro de los beneficios, la reducción de costos, el control de riesgos y en general la mejora de las operaciones de TI. Por tanto, hay que definir un Modelo de Proceso Integrado de Gobernanza y Gestión de TI, que abarcará la totalidad de los procesos que constituyen el ciclo de la información e integra las mejoras prácticas existentes para facilitar el trabajo de las organizaciones.

En el *Gráfico 4*, se adjunta un **Modelo de Gobierno Corporativo de Tecnologías de la Información** propuesto por Mark Toomey, donde podemos visualizar una versión evolucionada del modelo de ISO/IEC 38500 para el gobierno donde los tres pasos principales en el ciclo de gestión son reemplazados por las 08 disciplinas primarias claves (Estrategia, Arquitectura Empresarial, Cartera, Programa, Proyecto, Activo, Operación y Seguridad de Información) alineadas sobre los 4 primeros sistemas de gestión: Desarrollo Estratégico, Planificación, Implementación y Operación. En este camino, podemos ahora comenzar a desarrollar un mejor entendimiento de cómo se relacionan las tareas y roles de gobierno y gestión, y como son distintas e interdependientes.

Hemos visto por tanto, que la información, al ser uno de los principales activos de las organizaciones, debe protegerse a través de la implementación, mantenimiento y mejora de las medidas de seguridad para que cualquier empresa logre sus objetivos de negocio, garantice el cumplimiento legal, de prestigio y de imagen de la compañía.

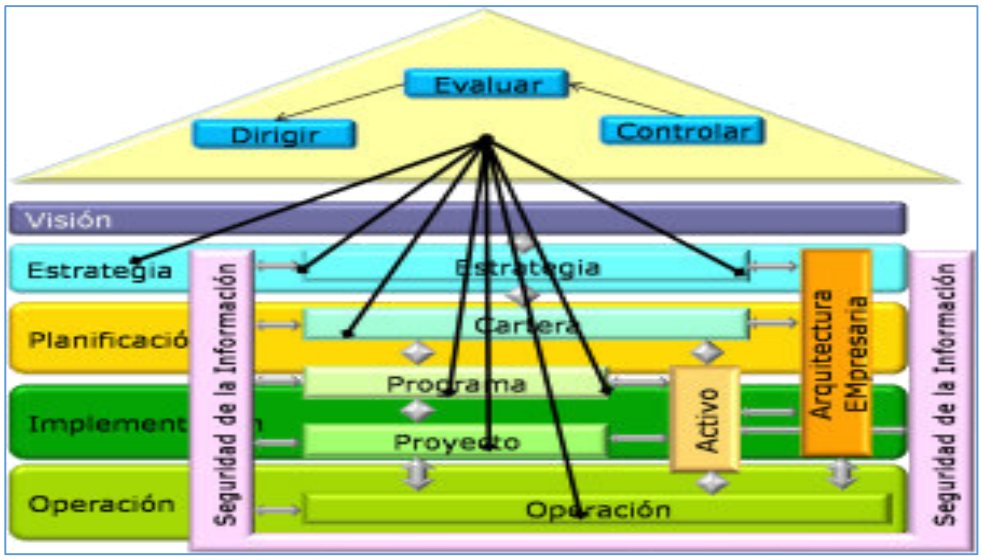


Gráfico N° 4: **Modelo del Gobierno Corporativo de Tecnologías de Información**
Fuente: **"Waltzing with elephants" - Mark Toomey**

Por otro lado, la Asociación Española de Normalización y Certificación (AENOR) ha desarrollado un **modelo de Gobierno y Gestión de las TIC** que está basado en estándares mundialmente aceptados, que nos permite visualizar la integración en la organización orientado a los objetivos empresariales y con una proyección de futuro.

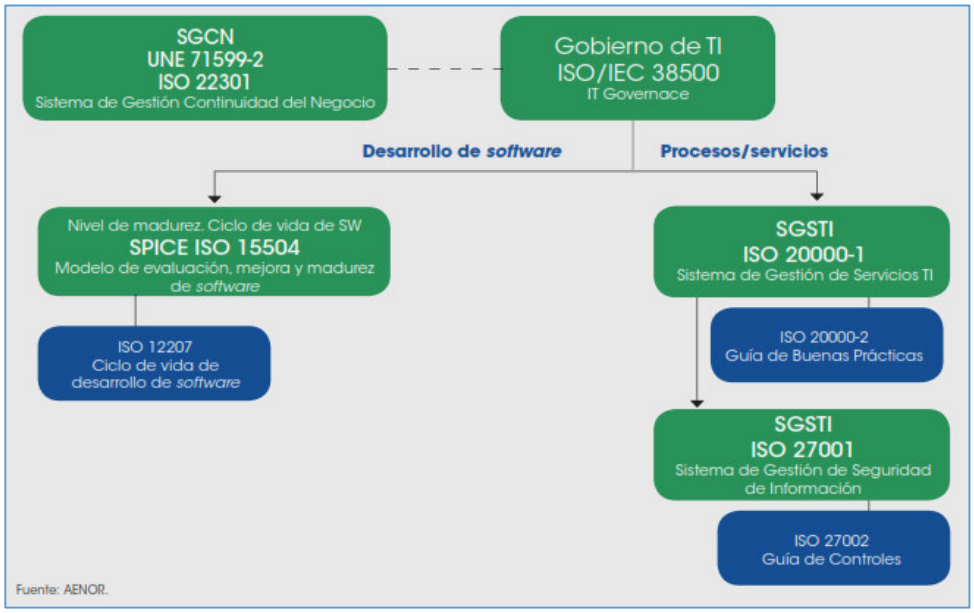


Gráfico N° 5: **Modelo integrado de Gobierno de TI con Normas y Estándares ISO**
Fuente: **AENOR**

Se hace necesario, por tanto, establecer estrategias respecto de la implementación del SGSI en la Administración Pública Peruana basadas en la ISO 27001 que estén más orientadas a dotar de una estructura organizacional de gestión de la información que permita el alineamiento de TI con la estrategia de negocios de las organizaciones, el logro de beneficios, la reducción de costos, el control de riesgos y en general la mejora de las operaciones de TI en las organizaciones.

2.4.2. Análisis de la Seguridad de la Información en el Perú

En el Perú, la Oficina Nacional de Gobierno Electrónico e Informática -ONGEI- ha venido emitiendo una serie de normatividades para desarrollar la implementación de la Seguridad de la Información de acuerdo a estándares internacionales, en el Estado Peruano.

Así, se aprobó en el año 2004, la Resolución Ministerial N° 224-2004-PCM, la primera versión de la ISO 17799; En el año 2007, esta Norma Técnica Peruana fue actualizada mediante la Resolución Ministerial N° 246-2007-PCM, y reforzada a través de la publicación de la ISO 27001 en el año 2012, mediante la Resolución Ministerial N° 129-2012-PCM. Recientemente, en enero del 2016, se ha revisado y actualizado la ISO 27001 a través de la Resolución Ministerial N° 004-2016-PCM **[38].**

Además, la recientemente aprobada Política Nacional de Gobierno Electrónico tiene entre sus objetivos estratégicos el de garantizar la Integridad, Confidencialidad y Disponibilidad de la Información en la Administración Pública mediante mecanismos de la Seguridad de la Información gestionada, así como articular los temas de ciber-seguridad del Estado. **[32][36]**

El Gobierno Electrónico es la oferta de servicios que brinda el estado a sus ciudadanos, utilizando las tecnologías de información, particularmente el internet, creando un gobierno más cercano, abierto y eficiente. Para ello, es indispensable que las Organizaciones del Estado sean conscientes de la necesidad de tener en cuenta aspectos como la ***confidencialidad, integridad, disponibilidad*** y autenticidad de la información **[31].**

La Política Nacional de Gobierno Electrónico en el Perú, tiene entre sus pilares, en el Objetivo N° 3: ***"Garantizar la integridad, confidencialidad y disponibilidad de la información en la Administración Pública mediante mecanismos de Seguridad de la Información gestionada, así como articular los mecanismos de ciber-seguridad del Estado"*** **[38].**

Es decir, se tiene que garantizar el uso adecuado y eficiente de la información procesada a través de uso de tecnologías de la información en el Estado mediante una eficiente y proactiva administración de la Seguridad de la Información Gestionada, teniendo presente los derechos fundamentales de la persona, la Protección de Datos Personales, Gobierno Abierto (Open Government) y el proceso de Modernización del Estado. Por ello, la seguridad de la información es parte fundamental de las iniciativas de Gobierno Electrónico a nivel mundial.

2.4.3. Análisis de los Indicadores de implementación de la Seguridad de la Información en el Perú y Latinoamérica

Según la VI Encuesta Nacional de Recursos Informáticos en la Administración (VI ENRIAP) realizada en el año 2007 (Pág. 34), de 576 entidades públicas, 124 (21%) habían iniciado la implementación del SGSI, mientras que no implementaron 452 (79%). **[43].**

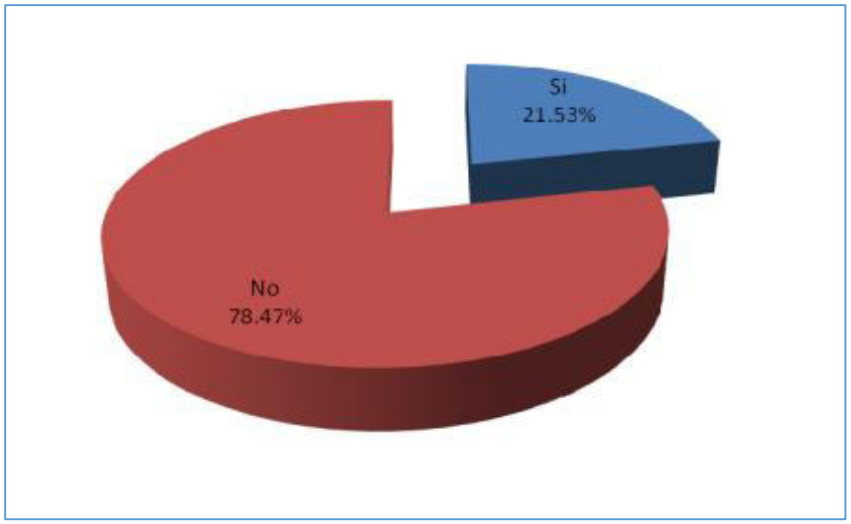


Gráfico N° 6 - **Porcentaje de Entidades Públicas que implementaron SGSI en 2007**
Fuente: **VI ENRIAP 2007**

Mientras que en la VIII ENRIAP del año 2010 (Pág. 75) **[44]**, de 552 entidades públicas, 182 (33%) habían iniciado la implementación del SGSI, mientras que las que no implementaron fueron 370 entidades públicas (67%). Podemos apreciar que existe un incremento de aproximadamente del 10% entre el 2007 y el 2010, lo cual sigue siendo un avance muy lento respecto de la implementación del SGSI en las instituciones públicas basado en la NTP 27001.

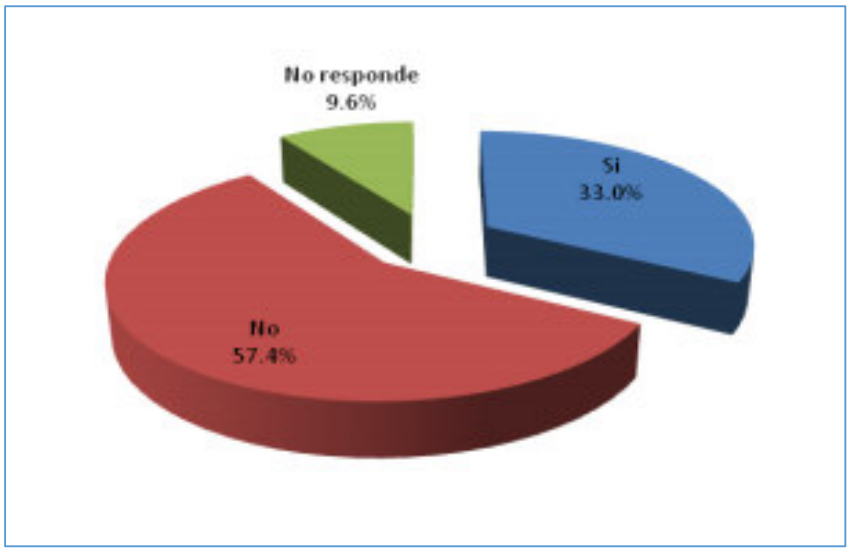


Gráfico N° 7 - **Porcentaje de Entidades Públicas que implementaron SGSI en 2010**
Fuente: **VIII ENRIAP 2010**

Por otro lado, según un estudio de JackSecurity del año 2008 (pág.12) respecto de los niveles de maduración de la Seguridad de Información en el Perú, se concluye que el Gobierno de la Seguridad de la Información se encuentra en un nivel de maduración "informal" de Nivel 2 según el modelo de maduración ITGI de 0 a 5.

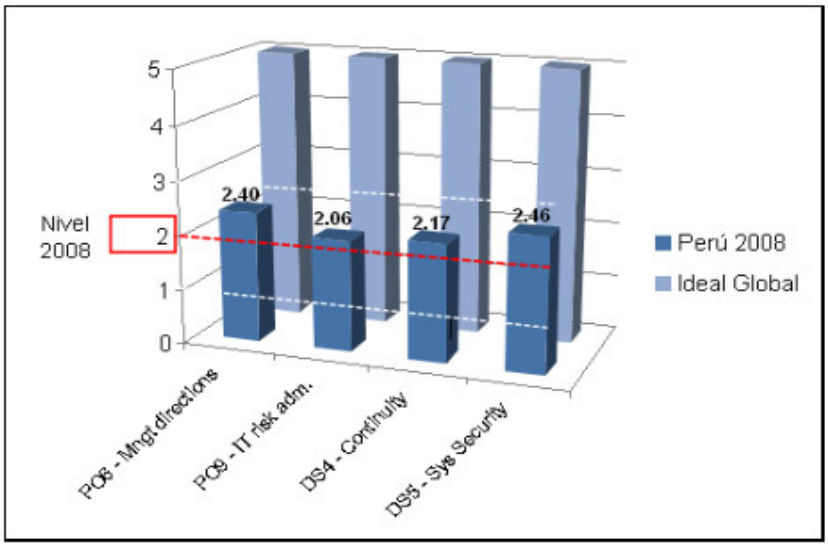


Gráfico N° 8: **Nivel de maduración ITGI 2008**.
Fuente: **Informe JackSecurity - nivel de maduración 2008**

Nivel de madurez 2 ITGI – repetible pero intutivo (Informal)

- ✓ Hay un entendimiento emergente de que los riesgos de TI son importantes y deben tenerse en cuenta.
- ✓ Existe un enfoque de la evaluación del riesgo, pero el proceso es aún inmaduro y en desarrollo.
- ✓ Las responsabilidades y la rendición de cuentas para la seguridad de la información son asignadas a un coordinador de seguridad de la información sin autoridad de gestión.
- ✓ La conciencia de seguridad está fragmentada y limitada.
- ✓ Los informes de Seguridad de la Información se generan, pero no se analizan.
- ✓ La seguridad tiende a responder de forma reactiva a los incidentes de seguridad de la información y mediante la adopción de las ofertas de terceros, sin abordar las necesidades específicas de la organización.
- ✓ Las políticas de seguridad se están desarrollando, pero se siguen utilizando las habilidades y herramientas inadecuadas.
- ✓ Los informes de seguridad de la información son incompletos, engañosos o no pertinentes.
- ✓ Se asigna la responsabilidad para el servicio continuo. Los enfoques de servicio continuo son fragmentados. Los informes sobre la disponibilidad del sistema son incompletos y no se tiene en cuenta el impacto en el negocio.

Si bien existe una comprensión emergente que los riesgos de TI en una organización son importantes y necesitan ser considerados, la evaluación del riesgo es aún inmadura y está en desarrollo. Además, las responsabilidades por la seguridad de la información son asignadas a un coordinador (oficial de seguridad de la información), pero sin autoridad gerencial.

Finalmente, la concientización de seguridad de información está fragmentada y limitada en las organizaciones (cultura organizacional casi nula).

Se puede afirmar también que muchas de las regulaciones pasadas y las aún vigentes no fuerzan directamente la relación de la "madurez" de los procesos de la seguridad de la información con una presencia supervisora de los agentes principales que componen el Gobierno, el comité de directorio y la alta gerencia de las organizaciones reguladas y normadas en el Perú.

Según un estudio realizado por KPMG en el año 2012, tenemos que el nivel de incidencia de fraude informático en el Perú es uno de los más altos de la región.

Este informe se realizó a partir de una encuesta de 73 empresas peruanas y filiales de firmas extranjeras en el Perú en el año 2012. **[27]**. El problema se presenta principalmente en el interior de las organizaciones (44% de las empresas encuestadas) y fue cometido por los niveles superiores pero también por empleados de menor jerarquía. De acuerdo a este informe, se puede observar que dentro de las modalidades de delito informático cometido, los principales fraudes se originaron en el robo de información confidencial (16%) y el robo de hardware (10%).

A nivel latinoamericano, según la IV Encuesta Latinoamericana de Seguridad de la Información, dentro de los estándares más utilizados en los últimos años está la ISO 27001, en la cual del 27% en el año 2010, pasó a un 56% en el 2012.

Con respecto a las normativas aprobadas por entes gubernamentales, pasó del 39% al 42% en los mismos años **[1].**

Los temas de cumplimiento vienen adquiriendo mayor importancia para las organizaciones, lo cual implica contar con herramientas que les permitan a las empresas peruanas movilizarse frente a los estándares internacionales.

ESTÁNDARES Y BUENAS PRÁCTICAS	2009	2010	2011	2012
ISO 27001	45.80%	27.37%	28.88%	55.83%
Common Criteria	5.20%	1.21%	3.65%	3.33%
Cobit 4.1	23.40%	14.88%	14.62%	31.11%
Magerit	5.20%	3.23%	2.74%	7.22%
Octave	2.30%	1.29%	2.19%	2.22%
Guías del NIST (National Institute of Standards and Technology) USA	12.30%	8.09%	7.49%	12.50%
Guías de la ENISA (European Network of Information Security Agency)	2.30%	9.70%	1.46%	1.94%
OSSTM - Open Standard Security Testing Model	7.50%	3.23%	4.38%	6.38%
ISM3 - Information Security Management Maturiy Model	3.90%	9.70%	1.46%	3.01%
ITIL	26.90%	17.47%	18.28%	40.27%
No se consideran	37.70%	10.19%	14.80%	21.38%
Otra;Top 20 de fallas de seguridad del SANS, ISO 17799. BS 259999, Cobit 5.0, NTC 5254, OWASP, ISSAF, PCI-DSS, MCIIEF, SOX, N4360, SARO, Comunicación A4609, Propias, Circular 052	7.10%	2.91%	-	6.94%

Tabla N° 2 – **Estándares y Buenas Prácticas de TI**
Fuente: IV Encuesta Latinoamericana de Seguridad de la Información 2012.ACIS

NORMAS Y REGULACIONES IMPLEMENTADAS	2009	2010	2011	2012
Ninguna	**52.30%**	**46.95%**	**42.94%**	38.05%
Regulaciones internacionales (SOX, BASILEA II)	15.60%	13.62%	17.05%	18.61%
Normativas aprobadas por entes de supervisión (Superintendencias, Ministerios o Institutos gubernamentales)	33.80%	39.42%	40.00%	**42.50%**
Otra: NTP ISO 17799, Contraloría General de Costa Rica, PCAOB, BASC, COMA 4609, PCI-DSS IOSA, SIGEN 48				5.27%

Tabla N° 3 – **Normas y Regulaciones implementadas de TI**
Fuente: IV Encuesta Latinoamericana de Seguridad de la Información 2012.ACIS

Finalmente, es de destacar también la Ley 26702 – Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica la Superintendencia de Banca y Seguros (SBS) que fija los criterios para una adecuada gestión de la seguridad de la información a través de la Circular N° G-140-2009, la cual obliga a todas las entidades financieras a establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI) tomando como referencia los estándares internacionales como el ISO 17799 e ISO 27001.

Esta norma, si bien es de obligatorio cumplimiento para las instituciones financieras del ámbito privado y AFP´s, también son de aplicación obligatoria para las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC).

De acuerdo a lo referido en esta Circular, las actividades mínimas que deben desarrollarse para implementar el SGSI, son las siguientes:

a. Definición de una política de seguridad de información aprobada por el Directorio.
b. Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.
c. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Así también estas empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información.

Finalmente, como parte de los informes periódicos sobre el riesgo operacional requeridos, emitido por la SBS, las empresas deberán incluir información sobre la gestión de la seguridad de la información. Además, la SBS podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión de la seguridad de la información de la empresa.

2.4.4. Análisis de la Seguridad de la Información a nivel mundial

La preocupación de las organizaciones por la seguridad de la información no debe estar centrada sólo en los aspectos más técnicos de la misma, sino que es necesario proponer a las entidades de sector público estrategias de gestión que abarquen el desarrollo, revisión y cumplimiento de las políticas de seguridad y abordar temas claves como la identificación de riesgos críticos, sensibilización, capacitación y privacidad.

En los últimos años la mayoría de los países de América Latina definieron estrategias, planes, políticas o programas digitales tendientes a poner en práctica políticas públicas en TIC, considerándolo como medios para el desarrollo de la sociedad en su conjunto. Para los países de la región, el llevar a cabo políticas públicas en este ámbito ha constituido un proceso de aprendizaje, que con más o menos altibajos continúa hasta el día de hoy.

Esta tarea implica la maduración y reformulación de las políticas tradicionalmente concebidas, para hacer frente a una temática altamente dinámica,

que impone retos a la gestión e institucionalidad pública, y que es afectada por distintos factores, tanto endógenos como exógenos a dicho proceso.

Con respecto a las políticas de gobierno, se tiene un estudio de CEPAL: "Políticas Públicas de la Sociedad de la Información en América Latina" **[21]**, en donde, de los 21 países de Iberoamérica para los cuales se cuenta con información, 16 de ellos se encuentran en el desarrollo de políticas digitales de primera generación y cinco de segunda generación.

A pesar del gran consenso regional sobre la relevancia de las TIC, a mediados de 2009 todavía es posible encontrar países que no cuentan con un documento de política. En efecto, en este documento se observa que ocho países están desde hace varios años en las primeras etapas de concepción y formulación de políticas de primera generación. En estos casos, es posible que una política haya sido acordada, sin embargo por uno u otro motivo ésta no se ha llevado a la práctica, haciendo que el proceso se estanque en su fase de formulación.

Otros ocho países están en la fase de ejecución de una primera generación de agendas digitales: Argentina, Colombia, Cuba, El Salvador, Guatemala, **Perú**, República Dominicana y Venezuela. Finalmente, los otros cinco (Chile, España, México, Portugal y Uruguay) están en la etapa de implementación de una segunda generación de políticas de TIC.

Si la región realmente quiere avanzar en el desarrollo digital debe trabajar por medio de políticas públicas que conjuguen elementos en dos niveles, estratégico y operativo, que consideren las particularidades de las TIC en tanto que objetivos de agenda de desarrollo.

Una estrategia de política en TIC debe contar con respaldo político que garantice su espacio dentro de la agenda pública de desarrollo, y le otorgue sustentabilidad y continuidad. Si bien los aspectos mencionados son denominadores comunes de toda política pública, en el caso de las TIC, por su característica transectorial y su vertiginosa dinámica tecnológica, se hace más necesario aún contar con una visión de estrategia de largo plazo que considere temas de complementariedades estructurales, a la que se apunte con un plan de acción de corto plazo. **[21]**

El Gobierno de Corea del Sur, desde 1970, logró compartir una visión nacional para construir una nación moderna, prepararse para el futuro y ser líder en la Sociedad de la Información **[42].** Actualmente, Corea del Sur se encuentra en la cima del ranking mundial de e-Government, o gobierno electrónico, que consiste en la utilización de las TIC para brindar mejores servicios a la sociedad y de paso mejorar la gestión de las instituciones públicas.

Esto responde a un plan integral para hacer que su gobierno sea más competitivo, lo que comenzó a idearse con la implantación del Sistema Nacional de Información Básica (NBIS), red que en 1990 se instaló en todas las instituciones públicas coreanas, para luego comenzar a idear un programa nacional más elaborado en el año 2000.

En dicho plan se concentraron en una primera etapa las "11 tareas para el gobierno electrónico" (2001 - 2002) y "31 tareas principales" (2003-2007) en una hoja de ruta que se cumplió a cabalidad y que ha dado resultados visibles: la eficiencia y transparencia en la labor administrativa se ha mejorado significativamente, los servicios administrativos son más eficientes y las oportunidades para que las personas participen en el proceso político se han

ampliado. Tras la interconexión y digitalización de todos los procesos del aparato público, Corea se enfocó en promover la convergencia de todos los servicios para maximizar la comodidad de los usuarios y la optimización del sistema de conexión digital entre departamentos y organismos gubernamentales, a fin de mejorar la calidad global y evitar fisuras.

En Corea del Sur, el trabajo manual en los organismos públicos ya no existe. Los ciudadanos pueden acceder a cualquier hora y en cualquier lugar a todos los servicios en línea que las entidades públicas ofrecen y todo el sistema se ha interconectado para mejorar la eficiencia y brindar el mejor servicio posible. Se ha creado el Ministerio de Administración Pública y Seguridad donde los trámites no requieren hoy de trámite físico alguno y el sistema ha demostrado ser tan eficaz que ya ha sido implementado en Vietnam y Costa Rica, mientras se estudia su puesta en marcha en diversos países emergentes como Ecuador y Kazajstán, que planean adoptar el modelo electrónico de correos.

Otra de las claves del éxito es que el uso de documentos electrónicos se ha convertido en práctica habitual en Corea y prácticamente la totalidad de los asuntos administrativos, como la gestión de personal, finanzas y adquisiciones se efectúan en línea. Además, todas las organizaciones de la Administración Central han introducido un sistema estandarizado de procesos denominado ***BPS On-nara*** (*) para registrar todos los procedimientos de decisión del gobierno, buscando aumentar la transparencia de la administración.

Además, poseen un **sistema seguro y a prueba de errores donde** el centro integrado del gobierno coreano gestiona globalmente todas las plataformas de información, lo que incrementa su capacidad para responder a los errores del sistema

y las amenazas de seguridad. Aunque en Corea están conscientes del éxito de su modelo, hay un trabajo constante para perfeccionarlo.

Es así como recientemente se trazaron cinco nuevas metas:

- **Gobierno electrónico portátil:** Se trabaja actualmente en facilitar el acceso a los trámites online por medio de dispositivos móviles.
- **Gobierno electrónico verde:** El gobierno coreano implementará la llamada "Oficina Verde", que promoverá la compra de equipos computacionales certificados como no contaminantes y que cuenten con tecnología de ahorro de electricidad.
- **Gobierno electrónico confiable:** Se está implementando un departamento especial que luchará contra los efectos negativos de la informatización, como la piratería, la filtración de información personal y la distribución de información ilegal.
- **Gobierno electrónico para todos:** Se trabajará además en facilitar el acceso al eGov de personas discapacitadas y ancianos, por medio de nuevas herramientas.
- **Gobierno electrónico global:** Corea no quiere guardarse su experiencia en torno al tema y se encuentra promoviendo su sistema en la comunidad internacional mediante la promoción de proyectos conjuntos con organizaciones internacionales y la exportación de plataformas de gobierno electrónico en diversos países.

> ***(*) BPS On-nara:*** *Se trata de un nuevo proceso de gestión empresarial que se basa en el manejo, registro y gestión de todos los procedimientos de trabajo de la administración pública de manera estandarizada y en línea.*
>
> *Las empresas y entidades de gobierno se clasifican de acuerdo sus funciones y objetivos, la creación de documentos y procedimientos de trabajo son uniformes y todos los procesos de toma de decisiones se registran para garantizar la rendición de cuentas y la transparencia de la administración pública.*

Finalmente, el e-Gov Coreano no sólo le da está dando satisfacciones al país en el ámbito interno. A raíz de su primer lugar en el ***United Nations E-Government Survey 2010***, Corea registró un importante aumento en exportaciones, debido principalmente a la intensificación del interés de empresarios de otros países por este sistema, que batalla por ser cada día aún más eficiente y transparente.

El Gobierno de Canadá, ha creado el Centro Canadiense de Respuestas a Incidentes Cibernéticos (CCIRC) **[5]** que es el órgano responsable de supervisar las amenazas y coordinar la respuesta nacional a cualquier incidente de seguridad cibernética cuyo objetivo es la protección de la infraestructura crítica nacional contra incidentes cibernéticos. Además, es parte de FIRST (Organización Internacional de Respuestas a Incidentes de Seguridad).

Por otro lado, se ha realizado una agrupación de especialistas de operaciones de TI en un solo grupo de trabajo nacional. Además, se ha creado el Área de Servicios Compartidos, que es un nuevo departamento creado en el 2011 con más de 6,000 funcionarios que realizan los siguientes servicios: 1) Consolidación de 485 Data Centers en solamente 7. 2) Migración de todos los sistemas de correo electrónico a una sola plataforma. 3) Creación de una única infraestructura de red de telecomunicaciones compartida.

En Uruguay**,** se vienen instrumentando políticas concretas para la administración pública en materia de Seguridad de la Información**.** Así, se ha creado por decreto gubernamental el Comité Nacional para la Sociedad de la Información (CNSI) que tiene la dirección ejecutiva de los planes para el desarrollo de la sociedad de la información **[37]**.

Sus cometidos, (atribuidos posteriormente a la AGESIC) son: 1) crear las condiciones para definir una política nacional concertada que permita el desarrollo de la sociedad de la información; y 2) Establecer los lineamientos generales para la definición de una Estrategia Nacional que tenga en cuenta la alfabetización temática, el desarrollo de servicios telemático, la modernización de la administración pública, promover el mercado de las telecomunicaciones e Internet y el desarrollo de condiciones de competitividad para el sector.

En el año 2005, el Presidente de la República Uruguayo crea un Grupo Honorario Asesor de la Presidencia en Tecnologías de la Información (GATI), con el propósito de formular una estrategia para la elaboración de una "Agenda Digital" que permitiera pautar el desarrollo tecnológico del país. Este grupo recomienda la creación de la "Agencia para el Desarrollo del Gobierno de Gestión Electrónica y de la Sociedad de la Información y del Conocimiento" (**AGESIC**). Dicha agencia tiene entre sus cometidos concebir y desarrollar una política nacional en temas de seguridad de la información. Con posterioridad la AGESIC establece la política de Seguridad de la Información para los organismos de la administración pública. Más adelante, en el año 2009 se establece que las unidades ejecutoras del presupuesto nacional, deben adoptar en forma obligatoria una política de seguridad de la información, tomando como base la que se incorpora por este decreto en su anexo, con propósito de impulsar un sistema de gestión de seguridad de la información (SGSI).

En Costa Rica**,** el Instituto de Normas Técnicas de Costa Rica (INTECO) ha realizado la emisión del estándar ISO/IEC 27000, desarrollando la norma INTE-ISO/IEC 27000:2010**.**

La Contraloría General de la República Costarricense se ha encargado de generar directrices y políticas en el tema de la Seguridad de la Información para las instituciones públicas **[33]**. Para ello, ha publicado la resolución "Normas Técnicas para la Gestión y Control de las tecnologías de Información". Dicha norma señala una serie de requerimientos generales de carácter institucional y acatamiento obligatorio, pretendiendo hacer viable la administración desconcentrada de las TIC, para lograr una mayor agilidad y oportunidad en el desarrollo de los proyectos y procesos informáticos. La norma se basa en algunos elementos de los estándares COBIT y el estándar internacional 27001.

Este estudio se realizó en base a 74 instituciones públicas pertenecientes al sistema bancario, ministerios del gobierno central y otras instituciones del estado. En las universidades se encuentran los mayores porcentajes de incidencia de eventos informáticos (presencia de virus), mientras que el menor evento que presentan las instituciones públicas es el robo de información digital o accesos sin autorización por parte de los empleados.

Sin embargo, del total de instituciones participantes, el 50% de ellas no cuenta con plan de continuidad de las operaciones dentro de su organización. A nivel público, las instituciones del sistema bancario son las que utilizan las mejores medidas de gestión de la seguridad, comunicaciones y manejo de contingencias. El seguimiento del plan de seguridad es el que menos desarrollan las instituciones públicas costarricenses.

El Gobierno de Taiwán viene impulsando fuertemente la política de seguridad nacional, cuya principal misión es promover y mejorar la implementación y certificación del SGSI **[29].** Además, el Gobierno también apoya la investigación

académica, imparte cursos educativos y promueve la certificación profesional. Además, se ha unido a muchas organizaciones de seguridad global. Así, en el 2001, se unieron al Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST), que es el mayor foro internacional de Seguridad de la Información.

En 2002, Taiwán se convirtió también en un miembro del equipo de Asia-Pacific Computer Emergency Response Team (APCERT).

Para mejorar la capacidad de investigación de los delitos cibernéticos, el Gobierno de Taiwán asistió a la 35ª reunión de detección de delitos informáticos para el Grupo de los Ocho (G8). Por otro lado, las principales entidades gubernamentales, incluyendo 37 departamentos públicos y 25 gobiernos locales, han establecido sus equipos de respuesta y designado a sus principales funcionarios de seguridad de la información para impulsar el plan de mecanismo.

El rango de clasificación de seguridad también se ha ampliado a casi 6,800 sectores públicos después de incluir las unidades educativas. Finalmente, más de 170 sectores públicos han acreditado la autenticación SGSI. El Centro Nacional de Operaciones de Seguridad (NSOC) también mejoró sus habilidades y proporciona protección de seguridad para las instituciones críticas durante todo el día.

La tasa de penetración de los sectores públicos se ha reducido de 1.2% a 0.84% en el 2005 y seguía disminuyendo gradualmente. Por supuesto, el Gobierno de Taiwán continuará mejorando la eficiencia de este plan y propagará sus esfuerzos de las unidades gubernamentales a las industrias y de las unidades básicas al sector público para asegurar la mejor utilización del SGSI.

Finalmente, se presenta la ***Encuesta Mundial de Certificaciones ISO 27001 del año 2013 y 2014***, elaborada por la International Organization for Standardization (ISO), y donde se puede notar que la gestión de seguridad de la información (ISO / IEC 27001) respecto de la tendencia del año anterior, presenta un crecimiento constante contando con un 14% de aumento en la certificación a nivel mundial.

En el *Grafico N° 9,* se ha hecho una comparación de la distribución mundial de la norma ISO/IEC 27001 certificados en el 2013 y 2014 donde se puede apreciar la marcada diferencia existente en países de Europa y Asia respecto de los países de Sudamérica.

Los tres principales países con el mayor número de certificaciones en el mundo son Japón, Reino Unido e India; mientras que, los tres primeros países que han crecido en el número de certificados en Sudamérica fueron Brasil, Colombia y Chile (que desplazó a Argentina en el 2014)

Gráfico N° 9 - **Certificación mundial ISO/IEC 27001 en los años 2013 y 2014**
Fuente: **ISO Survey 2013. Elaboración propia.**

2.4.5. Investigación sobre los factores que afectan la seguridad de la información a nivel mundial

A continuación, se presentan una serie de investigaciones que han estudiado los factores que afectan la seguridad de la información realizados a nivel mundial. Dichos estudios recogen las principales causas que se presentan al implementar la seguridad de la información en las organizaciones públicas y privadas de todo el mundo.

Estos estudios son los siguientes:

I) De acuerdo a un caso de estudio respecto de los ***"factores que influyen en la gestión de la seguridad de la información en empresas pequeñas y medianas en Turquía"*** [54], en donde se examinó la seguridad de la información empresarial en pequeñas y medianas empresas de ese país a través de encuestas, y luego se compararon los resultados con datos similares de diferentes países.

Esta encuesta fue realizada a oficiales de seguridad de la información e incluyó 09 secciones: política de seguridad, seguridad de la organización, clasificación de activos y control, seguridad personal, seguridad física y ambiental, comunicaciones y gestión de operaciones, control de acceso, desarrollo y mantenimiento de sistemas y gestión de continuidad de negocios.

<u>Conclusiones</u>

De acuerdo a los resultados que se obtuvieron de la investigación, se concluyó lo siguiente:

1°) Son factores importantes el apoyo que brindan tanto la Alta Dirección como los empleados a las políticas de seguridad de información institucional, así

como la obligación de todas las personas y empresas a cooperar en la conformación de dichas políticas.

2°) También es importante contratar especialistas de seguridad en el staff de la empresa que formen al personal técnico y directivo; aunque podría ser también la contratación de servicios de consultoría.

3°) Así también, se concluyó que cuando la Gestión de Comunicaciones y Operaciones y de Seguridad (Anexo A – Dominio A10 de la ISO/IEC 27001:2005) mejoran, otro parámetros de seguridad en las empresas mejorarán también (como los de organización, personal y de seguridad física)

II- En otra investigación respecto de la ***"política nacional de seguridad de la información y su aplicación: Un estudio de caso en Taiwan"*** [29], se estudian los diferentes factores claves para una implementación exitosa del SGSI. Para ello, se hace un análisis del estado actual de la seguridad de la información en Taiwán y luego se presenta un ejemplo exitoso de una entidad gubernamental que implementó el ISO 27001.

En el presente estudio se hace énfasis en la atención que viene prestando este país respecto de las políticas de seguridad de información en los últimos años. Es así que, hasta el momento se llevan gastado 250 millones de dólares en este proyecto principalmente en dos frentes:

1°) Desarrollar la capacidad de mantener la seguridad de sus redes de comunicación. Los sectores públicos deben luego monitorear y responder a los incidentes de seguridad mediante el uso de tecnologías avanzadas de información y mecanismos de gestión.

2°) Implementación de programas de concienciación y educación que permitan fortalecer la eficacia del sistema de seguridad de la información.

La principal misión de la política de seguridad nacional del Gobierno de Taiwán es promover y mejorar la implementación y certificación del SGSI. Es así que, hasta el momento, más de 3.700 sectores públicos han sido incluidos para salvaguardar sus sistemas de I&C. También se llevado a cabo más de 50 cursos y conferencias de formación, en los que se capacitó a casi 20.000 trabajadores relacionados con la seguridad. Asimismo, más de 200 servidores han sido galardonados con el certificado profesional de seguridad de información y 32 organizaciones públicas y privadas han adquirido la certificación internacional para la seguridad de información.

Para el diseño de este estudio, se eligió un caso de una organización pública que permitió estudiar cómo los departamentos llevan a cabo las políticas gubernamentales y cuáles son los factores críticos en la implementación del SGSI. La institución en estudio fue el "Centro de Transacciones de Acciones y Bonos de Taiwán", entidad perteneciente al Ministerio de Economía de este país.

Algo importante de destacar es que esta organización inició la implementación de la norma ISO 9001 en 1997, con el fin de elevar la calidad del servicio y fortalecer la eficiencia de la gestión, adquiriendo su respectiva certificación en marzo de 1998.

La investigación permitió conocer, por referencias de los directivos de la entidad, que debido a la experiencia en la ejecución de la ISO 9001, se tiene una clara comprensión de la implementación de un sistema de gestión en la organización. Cuando se comenzó la implementación del SGSI, esta entidad encontró, por

ejemplo, que el concepto de control de seguridad ya se había incorporado en muchas operaciones y procesos internos cuando se implementó la ISO 9001.

Finalmente, la investigación permitió encontrar los siguientes factores que han influido en la implementación del SGSI en esta organización, como son:

1- **La experiencia pasada de otras normas ISO**

   Con la experiencia pasada de la ISO 9001, el personal de esta organización ya estaba preparado para afrontar la ejecución del SGSI bajo la ISO 27001, debido a que la arquitectura y los procesos de aplicación de las normas 9001 y 27001 son consistentes.

2- **El nivel de documentación y estandarización**

   El gran número de documentos para la implementación del SGSI sigue siendo una pesada carga. Sin embargo, con la ejecución de la ISO 9001, se inició el establecimiento formal de la documentación.

   Es así que, durante la implementación de la ISO 9001, más del 70% de los procesos de la organización fueron bien documentados y podrían ser utilizados de nuevo para la implementación del SGSI.

3- **El procedimiento de evaluación de riesgos de activos**

   La evaluación de riesgos es el núcleo del SGSI, pero ésta no es una tarea fácil para la mayoría de las organizaciones. Es así que, al elegir la probabilidad de ocurrencia, los empleados no tienen idea de cómo decidir por una. No existe un método estándar diseñado para la evaluación de riesgos y las experiencias pasadas no ayudan mucho en la evaluación de riesgos.

4- **El apoyo de la Alta Dirección**

   Muchos investigadores han encontrado que este es uno de los factores más críticos que afectan el resultado de aplicación de las innovaciones que se

quieren realizar en una organización. Kankanhalli et al. (2003) ha demostrado que las organizaciones con fuerte apoyo de la dirección pueden participar más en esfuerzos preventivos. En este caso, el supervisor apoya firmemente en la ejecución debido a la exigencia gubernamental y su cumplimiento normativo.

Asimismo, los altos directivos y el comité de seguridad asistieron a los cursos de formación y se involucran en el establecimiento de la política de seguridad, la asignación de recursos, la planificación de horarios y la negociación de funciones cruzadas. Este apoyo demuestra la determinación de la alta dirección para todo el personal de la organización y proporciona los recursos necesarios para su ejecución.

5- La cultura de la organización

La cultura de seguridad de la información de una organización puede ser un factor importante para el mantenimiento de un nivel adecuado de seguridad de la información en esa organización. (Von Solms, 2000).

De acuerdo a los resultados de esta investigación, esta institución es agresiva en la adopción de nuevos sistemas tecnológicos y de gestión debido a su cultura organizacional, la cual es de una alta calidad; por lo que no es de extrañar que sea fácil y natural promover la implementación del SGSI en esta organización.

6- La conciencia de seguridad de la información y la educación

Muchos administradores de seguridad creen que la educación y la certificación son importantes para los profesionales y para una organización (Wade, 2005).

Otro informe concluye que la asignación de personal no capacitado para mantener la seguridad y la disponibilidad para ninguna formación al personal es un error importante que conduce a eventos de seguridad graves (Cortés, 2004).

En el caso de esta organización, ofrece cursos profesionales para capacitar a los miembros del comité de seguridad de la información y muchos otros empleados involucrados. Además se anuncia la política de seguridad de la información a todo el personal a través de documentos oficiales y carteles por todas partes.

Estas acciones disminuyen la resistencia de su implementación, por parte del personal del a institución, debido a la clara comprensión del objetivo de la organización respecto de la seguridad de la información.

Conclusión

Los resultados de este estudio indican que la experiencia pasada con éxito en otras normas, la disponibilidad de los documentos necesarios, el aprendizaje y la cultura organizacional son las principales motivaciones de una implementación exitosa del SGSI en una organización.

III- En un trabajo de tesis de una institución colombiana denominada ***"Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad financiera de segundo piso"*** [22], se han aplicado los diferentes requerimientos de la norma ISO 27001:2013 sobre una entidad financiera, lográndose obtener una serie de diagnósticos que permitieron establecer el nivel de madurez de esta organización respecto de la gestión de la seguridad de la información.

Entre los factores que se encontraron, producto de una auditoría realizada por la jefatura de control interno de la entidad al proceso de Gestión de Tecnología, están los siguientes:

1) **Falta de un gobierno de seguridad de la información en la entidad**

   - No existe una directriz a nivel gerencial sobre seguridad de la información
   - No existe una participación activa de la alta dirección.

2) **Inexistencia de una cultura de seguridad de la información en la entidad**

   - Falta de concienciación, apropiación y conocimiento en temas de seguridad por parte de todos los funcionarios de la Entidad.
   - No existe una cultura de mejora continua de seguridad de la información.
   - Falta de interés por parte de los funcionarios en temas de seguridad.
   - No existe una participación actividad de toda la organización con relación a la definición de procedimientos adecuados y a la planeación e identificación de controles de seguridad basados en una evaluación de riesgos
   - Los funcionarios no distinguen la diferencia entre seguridad informática y seguridad de la información.

3) **No existe un sistema de información adecuado para la gestión de riesgos de seguridad**

   - La entidad no cuenta con un sistema de información adecuado para la gestión de riesgos de seguridad.
   - No existe una valoración de riesgos de seguridad de TODOS los activos de información.
   - La entidad no cuenta con una visión global del estado de su seguridad, y por lo tanto no puede determinar con exactitud la efectividad de las medidas que sobre seguridad implemente.
   - Dificultad para el control y clasificación de los activos de información.
   - Inadecuada identificación de riesgos y controles de seguridad.

4) **La política de seguridad existente no está alineada con los objetivos del negocio**

- La política de seguridad existente no está alineada con las estrategias y objetivos del negocio.
- Las políticas de seguridad son definidas por la Dirección de Tecnología.
- Se requiere segregar las funciones de seguridad informática y seguridad de la información.

Conclusiones

Una de las principales recomendaciones de esta investigación es que, si no se consigue el compromiso demostrable de la Alta Directiva hacia la seguridad de la información, entonces no es recomendable implementar en las organizaciones un Sistema de Gestión de Seguridad de la Información.

Otras conclusiones del estudio son las siguientes:

- ✓ Es necesario el establecimiento de unas políticas de seguridad aprobadas por la Alta Dirección, para garantizar su debida implementación, actualización y cumplimiento.
- ✓ Se requiere implementar controles adecuados y efectivos, o fortalecer los existentes, con el objetivo de asegurar que la seguridad de la información sea parte del ciclo de vida del desarrollo de aplicaciones de la entidad
- ✓ Se requiere establecer un plan anual de capacitación, formación y sensibilización en seguridad de la información, con el objetivo de fortalecer la cultura de seguridad en los colaboradores y terceros que laboran para la entidad.
- ✓ Es fundamental que el oficial de seguridad participa en los comités de cambios.
- ✓ La entidad no tiene establecidos los lineamientos para el uso aceptable de los activos de información asociados con la información e instalaciones de procesamiento de información.

IV- En otro estudio denominado ***"Los 10 pecados capitales de la gestión de la seguridad de la información"*** [54], se identificaron aspectos esenciales, los cuales, si no se toman en cuenta en un plan de gobierno de la seguridad de la información, harán que dicho plan fracase o al menos causen graves fallas en el mismo. Entre los principales "pecados capitales" tenemos los siguientes:

1°) ***No darse cuenta de que la seguridad de la información es una responsabilidad del gobierno corporativo y tiene consecuencias legales.***

Hay que entender que l comprensión de la gobernabilidad en seguridad de la información es una parte esencial e integral del gobierno corporativo, la cual ha crecido específicamente en los últimos años.

Las consecuencias de cometer este pecado: la dirección ejecutiva no se está realizando y ejerciendo el debido cuidado, lo cual puede desembocar a graves responsabilidades directivas y personales.

2°) ***No darse cuenta de que la seguridad de la información es una cuestión de negocio y no un problema técnico.***

En muchos casos, la dirección ejecutiva en las empresas todavía piensa que la tecnología es todo lo que se requiere, y por lo tanto, se delega a los departamentos técnicos, y paulatinamente se olvidan de él.

Las consecuencias de cometer este pecado: el problema de seguridad de la información será enfocada en la tecnología únicamente, en lugar de una solución total integral. Esto también podría resultar en pérdida de dinero para la empresa.

3°) ***No darse cuenta de que un plan de seguridad de la información debe basarse en los riesgos identificados.***

El propósito de la seguridad de la información es proporcionar medidas para mitigar los riesgos asociados a los recursos de información de la empresa. Sin embargo, si ésta no tiene claro cuáles son sus amenazas potenciales, así como cuales son los bienes que debe proteger, es posible que, básicamente, camine en la oscuridad, y el gasto de dinero se realice para protegerse de amenazas que tengan una baja probabilidad de ocurrencia e ignorar otras que tienen un impacto muy grande una vez que ocurren.

Las consecuencias de cometer este pecado: la empresa puede estar gastando dinero en riesgos que pueden no ser realmente tan peligrosos, haciendo caso omiso de los demás que pueden ser muy graves.

4°) ***No darse cuenta de que es esencial una estructura (organización) de gobierno de seguridad de la información adecuada.***

Es esencial que una empresa deba contar con una estructura organizativa de seguridad de la información adecuada para hacer un plan de seguridad de la información exitoso. Esta estructura tiene que ver con la forma en que está organizada una empresa en seguridad de la información con códigos de buenas prácticas de seguridad. También incluye claridad sobre qué aspectos de seguridad de la información deben ser centralizados y qué aspectos deben ser descentralizados.

Las consecuencias de cometer este pecado: todo lo relacionado con la participación y la seguridad de la información se remite automáticamente al administrador de seguridad de la información (individual), el cual no es realmente el propietario de cualquier información, sólo el custodio.

Si los propietarios de información no están claramente definidos, surgirán riesgos graves.

5°) ***No darse cuenta de que es fundamental la conciencia de seguridad de la información entre los usuarios.***

No existen programas de sensibilización adecuados, y los usuarios no son conscientes de los riesgos del uso de la infraestructura informática de la empresa, y los posibles daños que pueden causar. Por otra parte, a menudo ni siquiera son conscientes de las políticas, procedimientos y normas de seguridad de la información existentes en la empresa.

Por ello, los usuarios no pueden ser considerados responsables de los problemas de seguridad si no se les dice lo que son este tipo de problemas de seguridad, y lo que deben hacer para prevenirlos.

Las consecuencias de cometer este pecado: muchas intenciones relacionadas con la seguridad de la información no podrán materializarse si los usuarios no están educados adecuadamente en este sentido.

V- En otro estudio analizado denominado: ***"Roles ejecutivos del comité de seguridad de la información"*** [55], se exploran los diferentes roles y responsabilidades que debería afrontar el Oficial de Seguridad de la Información y que contribuirán en una implementación exitosa.

En ese sentido, se analizan una serie de factores a tener en cuenta en la implementación, como son:

1°) **El proceso de integración**, se ha estudiado que existe una creciente necesidad de integrar funciones anteriormente responsables de aspectos específicos de la seguridad en una entidad holística capaz de reconocer,

prevenir y reaccionar ante cualquier amenaza a la información o a los activos dentro de una organización empresarial.

2°) **Las responsabilidades de seguridad de la información** se da a todos los niveles de la organización, teniendo en cuenta que si bien los especialistas en seguridad tienen la responsabilidad de diseñar, implementar y gestionar las medidas de seguridad específicas que la entidad vaya a necesitar, en última instancia es responsabilidad de cada uno de los empleados ayudar a garantizar la seguridad de la información en las organizaciones.

3°) **Existe un imperativo de seguridad de información**, el cual es de suma importancia para el comercio mundial. La seguridad es un proceso continuo donde el nivel de atención y el compromiso deben seguir siendo una prioridad en todo momento. Por esta razón, es esencial que las funciones y responsabilidades deben ser definidas y las estructuras organizativas sean diseñadas e implementadas correctamente.

4°) **Estructuras organizativas para la seguridad de la información**, las que pueden variar de una entidad a otra dependiendo de, entre otras cosas, el tamaño de la organización, la industria y la cultura. Una estructura típica reconoce la existencia de una de una función de riesgo corporativo centralizada. Sin embargo, lo más importante es la necesidad de un gobierno que será esencial para:

- Establecer responsabilidades claras de decisión
- Proporcionar un marco de garantía para permitir la transparencia de la actividad junto con las métricas adecuadas
- Asegurarse de que se cumplen los requisitos reglamentarios
- Ofrecer garantías del cumplimiento de los requisitos de negocio para la seguridad

- Asegurar que los recursos se utilizan de manera adecuada y prudente y que se está obteniendo relación calidad-precio.

5°) **El Comité de Auditoría,** el cual es fundamental para la eficacia de la gestión de la seguridad de la información en las organizaciones.

6°) **El papel del Oficial de Seguridad de la Información** (CISO), el cual ha sido tradicionalmente encasillado dentro de las funciones de TI. Sin embargo, ahora el CISO reporta a una función de negocio debido a que la mayoría de la información corporativa reside ahora dentro del ámbito digital y la protección de esta información es un requisito crítico. El nuevo énfasis estará en la comprensión más amplia de los riesgos de negocio y el contexto en el que la seguridad relacionada con TI tiene que coexistir.

7°) **El Jefe de Informática** (CIO), el cual tendrá una responsabilidad directa en la seguridad de la información en la medida en que se pueda gestionar desde dentro de ella. Por ahora, sigue siendo que el CISO reporta directamente al CIO.

El CIO también es responsable de asegurar que los miembros de la Alta Dirección y otros directivos de la empresa entiendan lo suficiente como para cumplir con las responsabilidades de gobierno de TI, incluidos los de seguridad.

8°) **El Director de RR.HH.**, en donde se sabe que los problemas de seguridad son causados en gran parte por personas y no por la infraestructura técnica. Por tanto, la función de recursos humanos puede ayudar a asegurar que las políticas de personal adecuadas, se establecen y se mantienen. Por ejemplo,

la formación de inducción para el nuevo personal debe incluir seguridad de la información.

Conclusión

En conclusión, el Oficial de Seguridad de la Información ya no puede soportar ser el único responsable de dicha seguridad. Hay muchas personas y muchos papeles dentro de una organización que deben compartir esta responsabilidad. El éxito será para aquellas organizaciones que reconocen estos roles definidos, establecer una responsabilidad clara y proporcionar la estructura de gobierno adecuada.

VI- En otro estudio de investigación denominado: ***"La política de seguridad de la información: un modelo de proceso a nivel organizacional"*** [26], se desarrolla un modelo de procesos de política de seguridad de la información de las organizaciones, basado en las respuestas de un grupo de más de 200 profesionales certificados en seguridad de la información (CISSP), de más de 25 países y de diversas industrias. El propósito de esta investigación es el de ofrecer un estudio exploratorio basado principalmente en técnicas cualitativas para describir un modelo de procesos de la política de seguridad de la información a nivel de organizaciones que sea integral.

La metodología de la investigación utilizada fue la de la teoría fundamentada (enfoque Glasser y Strauss, 1967), que implica una serie de pasos estructurados que incluyó la comparación sistemática de las unidades de datos y la construcción gradual de categorías que describen los fenómenos observados. Por lo tanto, la descripción de los fenómenos evoluciona directamente de los datos. En base a ello, y después de un número de iteraciones y nuevos exámenes de los datos, esta investigación clasificó la información de la siguiente manera:

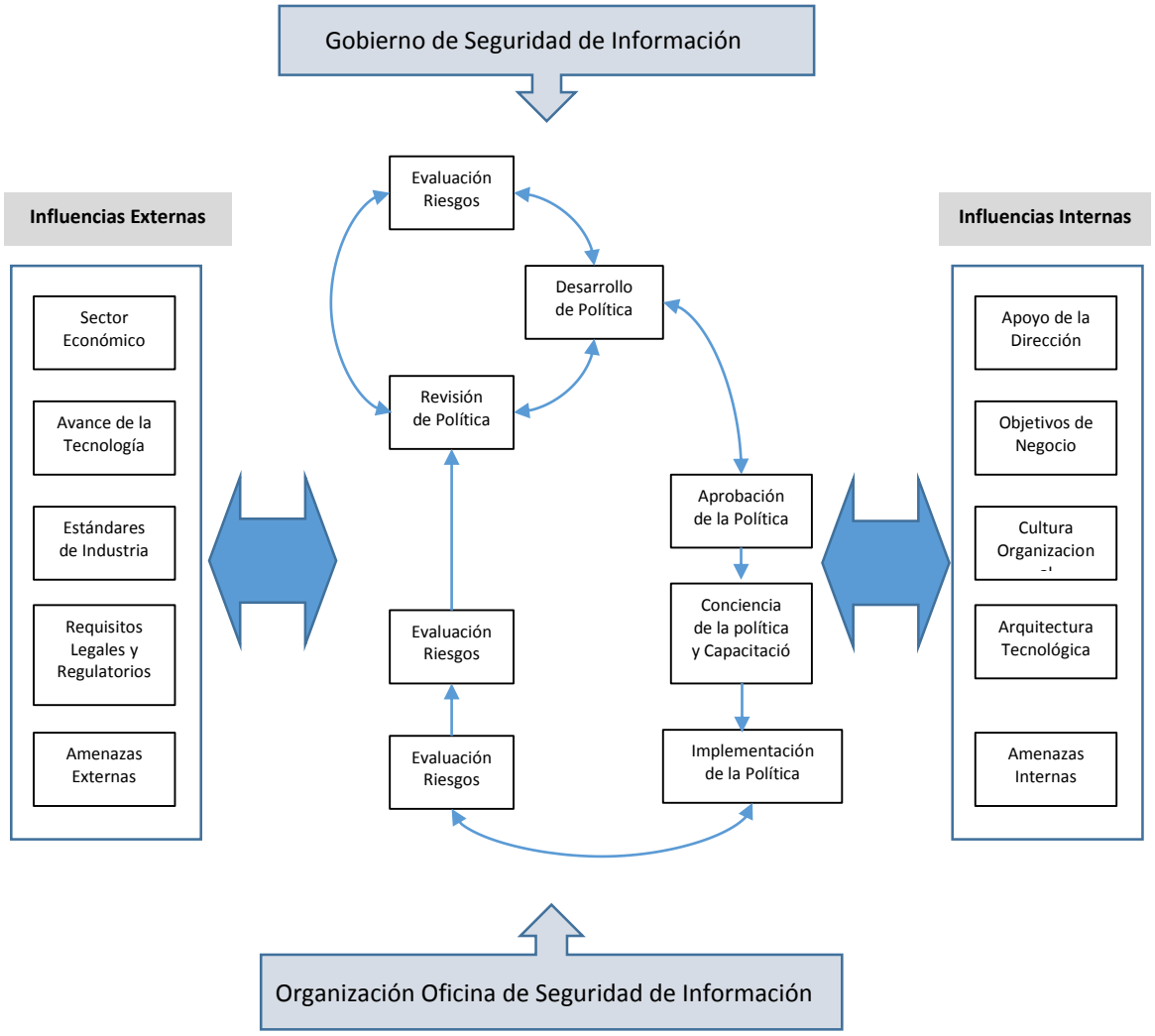
Clasificación	Categoría
1. Categorías Generales	1. Gobierno de Seguridad de la Información
	2. Organización de la Oficina de Seguridad de Información
2. Fases de Gestión de la Política	1. Evaluación de Riesgos
	2. Desarrollo de la Política
	3. Aprobación de la Política
	4. Conciencia de la Política y Capacitación
	5. Implementación de la Política
	6. Monitoreo (auditorías y herramientas automatizadas)
	7. Ejecución de la Política
	8. Revisión de la Política
3. Influencias Externas	1. Sector Económico
	2. Avances de la Tecnología
	3. Estándares de la Industria
	4. Requisitos Legales y Regulatorios
	5. Amenazas Externas
4. Influencias Internas	1. Apoyo de la Dirección
	2. Objetivos de negocios
	3. Cultura de la Organización
	4. Arquitectura Tecnológica
	5. Amenazas Internas

En esta investigación, se optó por no predefinir o suponer a priori ninguna de las categorías que se pueden encontrar en los datos. Por tanto, estas categorías describen las condiciones, eventos, experiencias y consecuencias asociadas con el desarrollo y gestión de las políticas de seguridad de la información. Es decir que, las categorías evolucionaron (según sus autores) directamente de la cantidad de respuestas de los participantes.

Resultados

El resultado de esta investigación arrojó un ***modelo de política de seguridad de información***, donde se muestra el flujo general de las clasificaciones encontradas y las principales interacciones entre las categorías identificadas en cada una de ellas.

El modelo resultante es el siguiente:



VII- Finalmente, se ha encontrado un trabajo de investigación en el Perú realizada en el 2010 denominado: **"Factores inhibidores en la implementación de sistemas de gestión de seguridad de la información basado en la NTP-ISO/IEC 17799 en la administración pública"** [31], en el cual se realizó un análisis cuantitativo respecto de las causas que han influido en el bajo nivel de implantación de la Norma Técnica Peruana NTP-ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática.

Esta investigación comprendió encuestas realizadas a 16 organismos públicos y cuyo análisis de los datos recopilados se ejecutó con el software estadístico SPSS 15.0.

Según el modelo de investigación y las hipótesis planteadas, se analizó la información recopilada, **primero**: Sobre el nivel de valoración que las instituciones objeto de la investigación le atribuyen a la norma; **segundo**: Sobre el proceso de implementación desarrollado; **tercero**: Sobre los factores críticos y su influencia en el cumplimiento de la implementación y, **por último**: Sobre el nivel de madurez o progreso alcanzado a la fecha de realización del estudio.

Conclusiones:

1°) Una de las primeras conclusiones obtenidas es que los organismos públicos descentralizados analizados, si valoran la importancia de la norma de seguridad para la institución. Sin embargo, esto no guarda relación con el nivel de implementación alcanzado.

2°) Se ha evidenciado dificultades, en las entidades encuestadas, para establecer un plan documentado de 01 o 03 años, así como la incorporación de dichos planes de seguridad en el Plan Operativo Institucional (POI) de cada una de ellas.

3°) De la revisión, que se realizó en esta investigación, respecto de los Planes Estratégicos publicados en el Portal de Transparencia de cada institución, se evidencia que no existe ninguna mención sobre la implementación de la norma como objetivo estratégico ni actividad relacionada. Esto confirma, según el análisis realizado, que la seguridad

de la información no está comprendido dentro del proceso de planificación estratégico que realizan dichas instituciones.

En consecuencia, no hay metas ni objetivos concretos a este nivel que se puedan reflejar con consistencia en el Plan Operativo y Presupuesto Institucional.

4°) No hay un entendimiento claro sobre la responsabilidad global de la seguridad de la información dentro de las Instituciones encuestadas. La implementación mayormente descansa en los gerentes o jefes del área de informática y sin el compromiso de la alta dirección.

5°) Por último, de la investigación realizada, también se percibe que en el proceso de implementación de la norma no hay un acompañamiento sistematizado del organismo rector como es la ONGEI a través de talleres o consultorías especializadas sobre la norma, tampoco un mecanismo de control para supervisar el desarrollo del mismo y sistematizar las lecciones aprendidas enmarcadas en un plan maestro de seguridad de la información de las entidades públicas.

2.5. Resumen

En este capítulo se ha desarrollado un análisis del rol fundamental que cumple la seguridad de la información en una organización. Además, se han analizado los indicadores tanto en el Perú como en Latinoamérica revisando el avance desarrollado a nivel mundial que permite identificar el estado actual de la seguridad de la información en el Perú, del cual se puede apreciar que entre los años 2007 y 2010 se ha logrado un incremento del 10% lo que sigue siendo un avance muy lento

respecto de la implementación del SGSI basado en la NTP 27001 en las instituciones públicas del Sistema Nacional de Informática del Estado Peruano.

Sin embargo, al compararlo con otros países de nuestra región, vemos que aún nos falta impulsar el desarrollo en materia de seguridad de información ya que países como Chile, Uruguay y México están entrando ya en una 2da. Generación de TIC en el Estado.

2.6. Definición de Términos

Seguridad de la Información. Preservar la confidencialidad, integridad y disponibilidad de la información; además, también pueden ser involucradas otras características como la autenticación, responsabilidad, no repudio y fiabilidad.

Sistema de Gestión de la Seguridad de la Información. SGSI. Es la parte del sistema integral de gestión, basado en un enfoque del riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Política Nacional de Gobierno Electrónico. Busca el uso efectivo de las Tecnologías de la Información y Comunicación-TIC, contribuyendo al proceso de modernización, descentralización y transparencia del Estado.

Protección de Datos Personales. Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no sólo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso.

Gobierno Abierto. Promover un Estado transparente y participativo donde gobierno y ciudadanos colaboran en el desarrollo colectivo de soluciones a los problemas de

interés público, a través de la implementación de plataformas de gestión de información e interacción social. Su finalidad es facilitar el acceso de los ciudadanos a los espacios de participación, transparencia y servicio que el Estado tiene disponibles para ellos, reuniéndolos en un solo lugar.

Gobierno Electrónico. Consiste en la implementación, desarrollo y aplicación de las herramientas informáticas tales como las tecnologías de la información y las comunicaciones. Implica la innovación en la reforma del Estado, involucrando el uso de la tecnología para agilizar procesos fomentar la competitividad del país y acercar el Estado a los ciudadanos.

De igual forma, se incluye su labor para impulsar la Sociedad de la Información y del Conocimiento.

Agenda Digital Peruana 2.0. Es el Plan de desarrollo de la Sociedad de la Información y el Conocimiento que tiene como objetivo general: "Permitir que la sociedad peruana acceda a los beneficios que brinda el desarrollo de las Tecnologías de la Información y Comunicación en todos sus aspectos".

ONGEl. La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), es el ente rector del Sistema Nacional de Informática encargado de proponer la Estrategia Nacional de Gobierno Electrónico, así como de coordinar y supervisar su implementación. Además coordina y supervisa la integración funcional de los sistemas informáticos del Estado y promueve el desarrollo de sistemas y aplicaciones de uso común en las entidades de la Administración Pública.

lSACA. La Asociación de Auditoría y Control de Sistemas de Información (ISACA), es una organización internacional que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información.

Es una fuente confiable de conocimiento, estándares, comunidad, y desarrollo de carrera para los profesionales en gobierno, privacidad, riesgos, seguridad, aseguramiento y auditoría de sistemas.

Es la entidad responsable de otorgar las certificaciones siguientes: CISA (Auditor Certificado de Sistemas de Información), CISM (Gerente Certificado de Seguridad de Información), CRISK y COBIT 5, entre otros.

2.7. Conclusiones

Se puede concluir de la revisión de la literatura que una estrategia de política en TIC debe contar con el respaldo político que garantice su espacio dentro de la agenda pública de desarrollo, y le otorgue sustentabilidad y continuidad.

Ahora, si bien muchos países -incluido el Perú- vienen impulsando entre sus políticas de gobierno a las Tecnologías de Información como parte de sus políticas públicas, es necesario también tener estrategias de continuidad de dichos programas.

La implementación de los Sistemas de Gestión de Seguridad de la Información en la Administración Pública, basados en la NTP-ISO/IEC 27001 debe estar orientado, por un lado, hacia el alineamiento de TI con los procesos de negocio de las Organizaciones y por el otro, hacia la cultura organizacional de las empresas. Existe una relación directa entre la efectividad de una estrategia de seguridad de la información y su cultura organizacional.

Por lo tanto, es importante trabajar en lo referente a la capacitación y profesionalización de expertos en seguridad de información que puedan conducir exitosamente planes estratégicos exitosos de implementación de SGSI en las entidades del sector público peruano.

CAPÍTULO 3 – METODOLOGÍA

En este capítulo se presenta el diseño de la estrategia de la tesis cualitativa, la cual está basada en la recolección de datos a través de herramientas tales como entrevistas y observaciones realizadas con el apoyo de propio investigador como instrumento principal.

Es decir, se explicará la forma de llevar a cabo la investigación para lograr responder a la pregunta de investigación. Para ello, se ha definido claramente el diseño de la investigación, la población objetivo, la unidad de análisis, el marco muestral y el tamaño de la muestra, así como la validez del instrumento (protocolo de la entrevista) para darle mayor confiabilidad al presente trabajo de investigación.

3.1. Tipo de Investigación

El tipo de investigación definido para el presente estudio califica como cualitativo, ya que tiene como objetivo la indagación descriptiva de los factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades de la Administración Pública según la NTP-ISO/IEC 27001. Además, la investigación es inductiva, ya que pretende obtener conclusiones generales a partir de los resultados obtenidos en el levantamiento de información de las entidades públicas de la muestra que se obtendrá, es decir, tendrá una perspectiva holística.

Asimismo, no pretende probar una hipótesis, por el contrario, pretende generar una; también deja abierta la posibilidad de incorporar variables o hallazgos que se encuentren en el proceso.

3.2. Hipótesis de la Investigación

La hipótesis son los supuestos que nos hemos planteado probar, indican lo que esperamos encontrar al dar respuesta a la interrogante central. En este sentido, Bernal Torres (2010, p.143) señala que la hipótesis es una suposición o solución anticipada al problema objeto de la investigación y, por tanto, la tarea del investigador debe orientarse a probar tal suposición o hipótesis. Aceptar una hipótesis como cierta no implica concluir respecto de la veracidad de los resultados obtenidos, sino que solo se aporta evidencia en su favor.

Para el presente trabajo de investigación, la hipótesis es la siguiente:

Hipótesis 1:

Las Entidades Públicas Peruanas enmarcadas en la NTP-ISO/IEC 27001 culminarán en forma efectiva la implementación integral del Sistema de Gestión de Seguridad de la Información.

Hipótesis 2:

La Oficina Nacional de Gobierno Electrónico e Informática -ONGEI- tendrá un rol protagónico como ente articulador y promotor de la implementación de la Norma Técnica Peruana referidas a la Seguridad de la Información ya que continuará liderando el Proyecto de Gobierno Electrónico en el Perú.

3.3. Diseño de la Investigación

El presente estudio de análisis cualitativo tiene un diseño basado en el método de la Teoría Fundamentada, el cual nos permite construir teorías, conceptos, hipótesis y proposiciones partiendo directamente de los datos y no de los supuestos a priori, o de otras investigaciones o de marcos teóricos existentes. La teoría generada se desarrolla inductivamente a partir de un conjunto de datos. El objetivo de la Teoría Fundamentada es, por tanto, el descubrimiento de una teoría explicativa comprensiva acerca de un fenómeno en particular.

El poder explicativo de la Teoría Fundamentada está en desarrollar la habilidad de poder explicar un suceso, por ejemplo explicar qué podría ocurrir en un negocio, o a un empresario, a partir de incidentes procedentes del campo de estudio.

Por tanto, la presente investigación realizada tiene las siguientes características:

a) Por su estrategia técnico-metodológica, **la investigación es cualitativa** porque pretende identificar los factores que dificultan, a las entidades de la administración pública peruana, la implementación del Sistema de Gestión de Seguridad de la Información según la NTP-ISO/IEC 27001.

b) Por su finalidad, **la investigación es básica** porque pretende desarrollar una teoría respecto de las dificultades encontradas en la implementación del SGSI -según la NTP ISO/IEC 27001- en las entidades públicas.

c) Por los objetivos, **la investigación es descriptiva** porque pretende relatar cuáles son los factores que afectan la implementación de los Sistemas de Gestión de Seguridad de la Información.

d) Por los tipos de datos que se trabajarán, **éstos serán primarios** porque para identificar los factores que dificultan la implementación del SGSI en las entidades de la administración pública peruana se realizaron entrevistas que nos permitieron levantar información de primera mano.

e) Por el grado de control, **la investigación es no experimental** porque no podríamos controlar todas las variables identificadas.

f) Por la secuencia temporal, **la investigación es transversal** porque la investigación no se realizará en distintos momentos para luego ver su evolución, esta investigación se realizará en un solo periodo de tiempo (sincrónico).

3.3.1. Población Objetivo

La población objetivo para este proyecto de investigación abarca a los Organismos Públicos Descentralizados que conforman el Sistema Nacional de Informática adscritos a la Presidencia del Consejo de Ministros (PCM) del Gobierno Central.

La Presidencia del Consejo de Ministros (PCM) es el organismo responsable de la coordinación de las políticas nacionales y sectoriales del Poder Ejecutivo. Coordina las relaciones con los demás Poderes del Estado, los organismos constitucionales, gobiernos regionales, gobiernos locales y la sociedad civil.

La PCM está compuesta por ***los Ministerios***, que comprenden uno o varios sectores considerando su homogeneidad y finalidad; y por las ***Entidades Públicas Desconcertadas***, las cuales están adscritas a un ministerio y son de dos tipos: Organismos Públicos Ejecutores y Organismos Públicos Especializados.

A continuación, en el *Gráfico N° 10* se presenta el Organigrama de las Entidades Públicas del Estado Peruano, el cual contiene a las entidades del sector

público, integrantes del Sistema Nacional de Informática, que deben implementar el Sistema de Gestión de Seguridad de la Información según la NTP-ISO/IEC 27001:2014, de acuerdo a lo establecido en la R.M. N° 004-2016-PCM. (En el *Anexo N° 7* se adjunta la norma de la referencia).

El Sistema Nacional de Informática fue creado por Decreto Legislativo N° 604, con el fin de organizar las actividades y proyectos que en materia de informática realizan las instituciones públicas del Estado Peruano, así como su relación con otros sistemas y áreas de la administración pública.

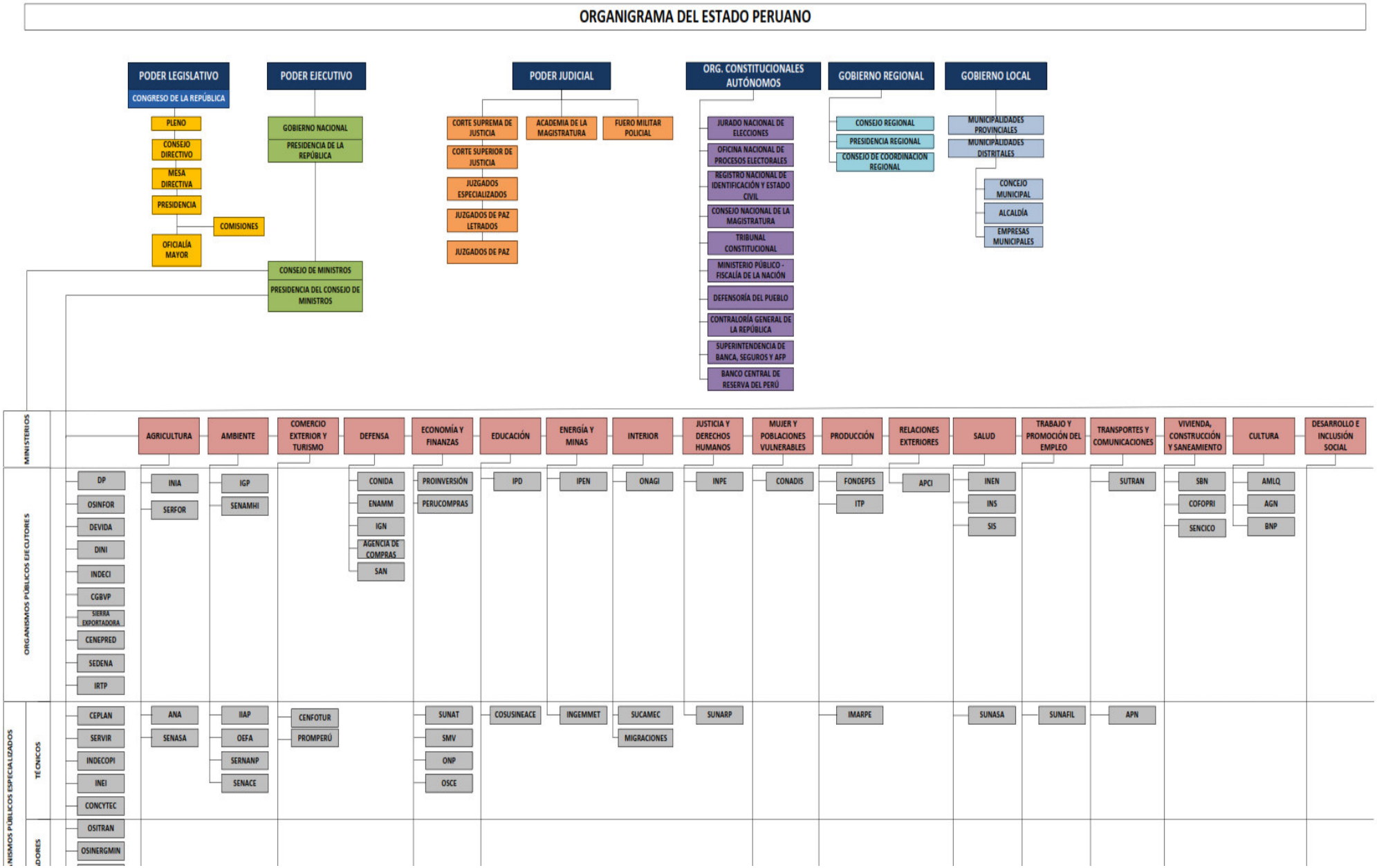
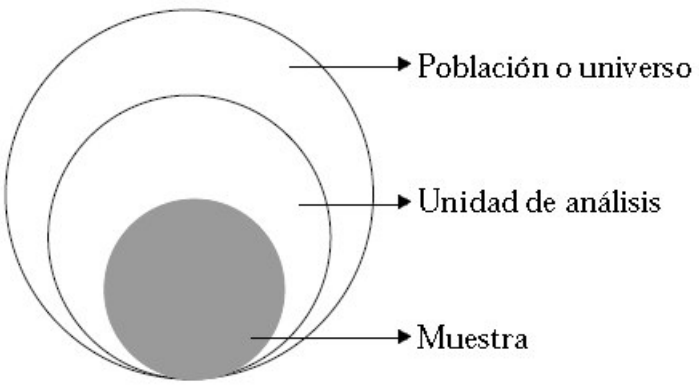


Gráfico N° 10: Organigrama de las Entidades Públicas del Estado Peruano

Fuente: Portal del Estado Peruano (http://www.peru.gob.pe/docs/estado.pdf)

3.3.2. Unidad de Análisis

La unidad de análisis para la presente investigación está compuesta por los Directores/Gerentes del Área de Informática o de los Oficiales de Seguridad de la Información de las entidades responsables de la implementación del Sistema de Gestión de Seguridad de la Información que son de cumplimiento obligatorio según la NTP-ISO/IEC 27001:2014.



Del Estudio de Investigación

Población o Universo
Entidades Públicas del Estado Peruano

Unidad de Análisis
Entidades Públicas en el marco de la NTP-ISO/IEC 27001:2014 (R.M. N° 004-2016-PCM)

Muestra
07 Entidades Públicas del Sistema Nacional de Informática en el marco de la NTP-ISO/IEC 27001:2014.

Gráfico N° 11 – **Diagrama de Población, Unidad de Análisis y Muestra**
Fuente: **Preparación de un proyecto de investigación (2003)**
(http://www.scielo.cl/pdf/cienf/v9n2/art03.pdf)

3.3.3. Marco Muestral

En esta investigación se ha optado por elegir muestras homogéneas que comprenden al personal de nivel gerencial o con el cargo de oficial de seguridad de la información de las instituciones representativas del Estado que, según la R.M. N° 004-2016-PCM, deben cumplir obligatoriamente con la implementación del SGSI de acuerdo a la NTP vigente.

Para el tamaño de la muestra elegido en esta investigación, se ha tomado como referencia el tamaño mínimo de muestra sugerido en los "casos de estudio en profundidad", de acuerdo a la tabla referencial de los tamaños de muestra comunes

en los estudios cualitativos citado por Hernández Sampieri, Fernández y Baptista (2010: p.395).

Tipo de estudio	Tamaño mínimo de muestra sugerido
Etnográfico, teoría fundamentada, entrevistas, observaciones.	30 a 50 casos
Historia de vida familiar.	Toda la familia, cada miembro es un caso.
Biografía.	El sujeto de estudio (si vive) y el mayor número de personas vinculadas a él, incluyendo críticos.
Estudio de casos en profundidad.	6 a 10 casos.
Estudio de caso.	Uno a varios casos.
Grupos de enfoque.	Siete a 10 casos por grupo, cuatro grupos por cierto tipo de población.

Tabla N° 4 - Tamaños de muestra comunes en estudios cualitativos
Fuente: Metodología de la Investigación (2010)- Hernández Sampieri-Fernández-Baptista

De acuerdo a lo especificado en la tabla de muestras para los estudios de casos en profundidad, se han seleccionado 07 Instituciones del Estado que han participado de la entrevista de investigación propuesta tomando en cuenta que están dentro de la relación de entidades solicitadas en la R.M. 004-2016-PCM (anexo N° 7). Para llevar a cabo la selección, se tomó en cuenta una mixtura de situaciones entre entidades públicas donde aún su implementación es inicial y otras que ya han desarrollado dicha implementación.

Estas entidades públicas son las siguientes: 1) Ministerio de Relaciones Exteriores - **RR.EE**, 2) Registro Nacional de Identificación y Estado Civil - **RENIEC**, 3) Instituto del Mar del Perú - **IMARPE**, 4) Oficina Nacional de Procesos Electorales - **ONPE**, 5) Ministerio Público - Fiscalía de la Nación - **MPFN**, 6) Ministerio de Economía y Finanzas - **MEF** y 7) Ministerio de Cultura – **CULTURA**

3.4. Consentimiento Informado

Se ha considerado conveniente para la investigación, hacer llegar una carta informando la naturaleza de la investigación con el fin de cumplir con el consentimiento informado.

Con este fin, se ha tomado como modelo el formato de consentimiento informado para participantes en proyectos de investigación definido por el Comité Permanente de Ética del Departamento de Psicología de la PUCP, ya que este cumple con las características mínimas para informar a los entrevistados el propósito del estudio de investigación, las condiciones de la entrevista y facilidades a brindar.

En el ***Anexo 1*** se adjunta el ***formato de consentimiento informado*** para esta investigación.

3.5. Confidencialidad

Los datos que pudiesen identificar a los participantes de las entrevistas personales son mantenidos en estricta reserva, guardando total confidencialidad de la información obtenida en las mismas.

En el ***Anexo 2*** se adjunta ***la carta de confidencialidad*** de la presente investigación, donde se manifiesta el compromiso de guardar total reserva respecto de la información obtenida de la entrevista efectuada, la misma que sólo será utilizada para el sustento y actividades necesarias dentro de la investigación.

3.6. Ubicación Geográfica

La investigación se realizará en las instituciones públicas del Perú más representativas responsables de la implementación del Sistema de Gestión de Seguridad de la Información que son de cumplimiento obligatorio según la NTP-ISO/IEC 27001, y que están ubicadas en la ciudad de Lima.

3.7. Instrumentación

El principal instrumento utilizado para realizar el proceso de levantamiento de información primaria es ***LA ENTREVISTA***. En este tipo de investigaciones, la herramienta primordial en la recolección de los datos es el propio investigador, constituyéndose en la característica fundamental del proceso cualitativo (Hernández-Sampieri, Fernandez y Baptista, 2010:p. 409), ya que a través de diversos métodos o técnicas, es éste el que recoge los datos, los analiza y, asimismo, es el mejor medio de obtención de información.

En esta investigación, se van a realizar principalmente entrevistas a profundidad, lo que permitirá entender cuáles son las restricciones o facilidades que encuentran los Gerentes de Informática (o los Oficiales de Seguridad de la Información) de las entidades responsables de implementar el Sistema de Gestión de Seguridad de la Información en las entidades de la Administración Pública Peruana, de acuerdo a la NTP-ISO/IEC 27001:2014.

En el ***Anexo 3*** se adjunta el ***protocolo de preguntas*** utilizado en las entrevistas realizadas. Este protocolo consiste en desarrollar una lista de áreas generales que deben cubrirse con el fin de asegurar que los temas claves sean explorados con cada informante. Es un instrumento que sirve para recordar los temas claves a preguntar.

Esta guía puede ser ampliada o revisada a medida que se van realizando las entrevistas.

3.8. Técnica de Recolección de Datos

En la recolección de datos existen diferentes técnicas que suministren la información adecuada. Algunas de estas técnicas son: la observación, encuestas, cuestionarios, entrevistas y sondeos.

Méndez (1999, p.143) define a las fuentes y técnicas para recolección de información como los hechos o documentos a los que acude el investigador y que le permiten tener información.

Hernández *et al* (2010) señala que la recolección de datos implica tres actividades que se encuentran estrechamente vinculadas entre sí, las cuales son:

- Seleccionar un instrumento o método de recolección de datos.
- Aplicar ese instrumento o método para recolectar datos.
- Preparar observaciones, registros y mediciones obtenidas.

Para la presente investigación, se ha utilizado la técnica de **entrevistas**, las cuales fueron de tipo semiestructuradas, ya que se dispone de un "guión" que recoge los temas que se deben tratar a lo largo de la entrevista. Sin embargo, el orden en el que fueron abordados los diversos temas y el modo de formular las preguntas se dejaron a la libre decisión y valoración del entrevistador.

Las entrevistas fueron realizadas bajo el siguiente esquema (Hernández, 2010:423): Contactar con el entrevistado, preparar una entrevista abierta o poco estructurada, ensayar la guía de entrevista con algún amigo, confirmar la entrevista un día antes, acudir puntual a la entrevista, vestirse apropiadamente y llevar el

formato de consentimiento informado y la *carta de confidencialidad* de la información obtenida. Así también, se utilizó el *protocolo de preguntas de la entrevista*, lo que permitió llevar el control sobre la entrevista y recoger la información relevante para dicha investigación.

Finalmente, se utilizaron herramientas propias de una entrevista tales como la utilización de una grabadora (con el consentimiento y autorización del entrevistado), así como lápiz y papel que permitió registrar la información relevante en la investigación.

En forma complementaria a las herramientas de recolección de datos, se está adjuntando -en anexos- una ***lista de recomendaciones a tener en cuenta al realizar las entrevistas*** en el ***Anexo 4***, así como también un ***esquema general de planeación de una entrevista cualitativa*** en el ***Anexo 5***.

Las coordinaciones para dichas entrevistas han sido acordadas, inicialmente, vía telefónica. Posteriormente, se realizaron visitas "in situ" al personal especialista en las instituciones señaladas para solicitar formalmente su apoyo y colaboración y poder llevar a cabo el trabajo de investigación propuesto. En algunos otros casos, se ha confirmado su participación a través de correos electrónicos De cualquiera de estas formas, han sido enviadas (y llenadas) las siguientes documentaciones:

a) Formato de consentimiento informado para participantes de la investigación (anexo 1)
b) Carta de confidencialidad de la información obtenida (anexo 2).

Las entrevistas serán semiestructuradas, ya que si bien están basadas en una guía de preguntas, se pueden ir introduciendo preguntas adicionales que permitirán precisar conceptos u obtener mayor información en detalle sobre el trabajo de investigación.

3.9. Validez y Confiabilidad del Instrumento

La confiabilidad y la validez son cualidades esenciales que deben estar presentes en todos los instrumentos de carácter científico para la recolección de datos. Según Pérez (1998:71), si el instrumento o instrumentos reúnen estos requisitos habrá cierta garantía de los resultados obtenidos en un determinado estudio y, por lo tanto, las conclusiones pueden ser creíbles y merecedoras de una mayor confianza.

Según Aroca, A. (1999: 269), el método que más se utiliza para estimar la validez de contenido es el denominado Juicio de Expertos, el cual consiste en seleccionar un número impar (3 o 5) de jueces (personas expertas o muy conocedoras del problema o asunto que se investiga), quienes tienen la labor de leer, evaluar y corregir cada uno de los ítems del instrumento para que los mismos se adecuen directamente con cada uno de los objetivos de la investigación propuestos.

De acuerdo con las reflexiones de la autora antes citada, se consideran expertos o jueces aquellos sujetos que reúnan las siguientes consideraciones:

a.- Formación académica en el área y rama objeto de la investigación

b.- Comprobada trayectoria experiencial de investigaciones realizadas en institutos y centros destinados para fines bien definidos;

c.- Desarrollo de una línea (o líneas) de investigación relacionada a intereses académicos;

d.- Poseer una amplia concepción epistemológica de la ciencia y de la investigación; y,

e.- Demostrar pleno dominio de la lengua castellana, pues la sintaxis, la semántica y la sindéresis son aspectos determinantes para dar forma interna y externa al instrumento.

Por tanto, para proceder a la validación por juicio de expertos del presente estudio de investigación, se procedió a elaborar una guía operativa a dichos especialistas, quienes lo emplean para evaluar y valorar la primera versión del instrumento de recolección de datos. En ella, se procedió a explicar el propósito del trabajo de investigación, así como de la importancia de la validez de dicho instrumento de recolección de datos por parte de su Juicio Experto para los fines específicos de la investigación. Además, se solicitaron los datos personales y profesionales del experto a entrevistar, tal como Nombre y Apellido, Documento de Identidad, Institución donde trabaja, Título(s) de Pregrado, Título(s) de Postgrado, Publicaciones y Certificaciones obtenidas (si las tiene).

3.10. Resumen

Según el diseño definido en el presente capítulo, la investigación *fue cualitativa y explicativa*, ya que pretendió identificar los factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades de la Administración Pública según la NTP ISO/IEC 27001; *fue transversal* porque la investigación tomó datos en un solo periodo de tiempo.

Debido a que la investigación fue desarrollada utilizando el método cualitativo, se ha utilizado a *la entrevista* como la herramienta principal para realizar el proceso de levantamiento de información primaria.

Como ya se ha referido en el presente trabajo, la característica fundamental en el proceso cualitativo lo constituye el propio investigador; por tal motivo, aunque este se basa en diferentes técnicas y herramientas de recolección de datos, el análisis y los resultados fueron inherentes a la persona que realizó el presente estudio de investigación.

CAPITULO 4 - ANÁLISIS DE DATOS Y DISCUSIÓN

Este capítulo tiene como finalidad presentar en detalle los datos recolectados durante el estudio de investigación, el análisis efectuado a los mismos, la estructuración realizada y finalmente la obtención de resultados de cada una de las entrevistas realizadas bajo la metodología cualitativa.

En el desarrollo del presente estudio, y al tratarse de una investigación cualitativa, se ha considerado la estrecha vinculación existente entre la recolección de datos y su análisis, los cuales ocurren en forma paralela **[51]**. Para la recolección de los datos, se ha utilizado a ***la entrevista en profundidad*** como herramienta de trabajo, la cual ha sido realizada a los oficiales de seguridad de la información encargados de su implementación en las Instituciones del Estado; mientras que para el análisis de los datos se procedió a un trabajo de ***codificación y categorización de la información***, con la finalidad de encontrar las restricciones que vienen afectando la implementación del sistema de gestión de seguridad de la información en las instituciones públicas.

4.1. Recolección de datos de la investigación

La recolección de datos, desde el enfoque cualitativo, es buscar datos que se convertirán posteriormente en información. Por tanto, en el proceso de recolección de datos de esta investigación se realizaron entrevistas a profundidad, que permitió obtener una diversidad de datos no estructurados y que progresivamente se han ido ordenando y estructurando.

4.1.1. Búsqueda de especialistas para la investigación

Para llevar a cabo dichas entrevistas era necesario encontrar especialistas de la unidad de análisis a investigar. Por tanto, el primer paso fue realizar una exhaustiva búsqueda de Oficiales de Seguridad de la Información en las entidades públicas, lo que fue realizado a través de diferentes instancias, como por ejemplo a través de ISACA, organismo de nivel internacional que certifica a especialistas en seguridad de la información, del cual se consiguió asociarse para un mayor acercamiento a los mismos y una mejor comprensión del ámbito de la investigación; así como también se realizaron contactos a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) como ente rector de la Política de Gobierno Electrónico del Estado Peruano.

4.1.2. Explicación de la investigación a los especialistas a entrevistar

Una vez efectuados los contactos necesarios, se inicia la etapa de convencimiento y explicación de la importancia del trabajo de investigación que se lleva a cabo. Para ello se preparó una ayuda memoria para la persona contactada que explica en forma concisa el propósito de la investigación, el problema a desarrollar

en la tesis, la unidad de análisis y el protocolo de preguntas; de tal manera que el entrevistado tuviera un panorama claro de lo que se quiere investigar y decidiera participar en la misma. En el **Anexo 6**, se adjunta una ***copia de la ayuda memoria para el entrevistado***.

4.1.3. Estructura del protocolo de preguntas de la investigación

Luego se realizaron las invitaciones oficiales al personal identificado. Dichas invitaciones fueron, en principio, efectuadas en forma presencial y posteriormente a través de correos electrónicos llevándose una bitácora de seguimiento de los entrevistados en el estudio de investigación para un mejor monitoreo y seguimiento del mismo, así como una relación de las invitaciones realizadas por correo.

Paralelamente a las coordinaciones efectuadas, se elaboró el protocolo de preguntas para realizar las entrevistas a profundidad (Anexo 3). Dicha herramienta fue organizada en 03 dimensiones, las cuales proporcionaron un mejor ordenamiento de ideas y un mayor desarrollo de las preguntas a realizar: Dimensión Técnica, Dimensión del Proyecto y Dimensión Institucional.

En el caso de la Dimensión Técnica, las preguntas estaban referidas al nivel de experiencia profesional que tiene el entrevistado respecto del estudio de investigación. Esta dimensión, nos permitirá conocer el grado y preparación técnica de la persona que responde la entrevista, así como darle un mayor nivel de profesionalidad a la investigación.

En el caso de la Dimensión del Proyecto, las preguntas estaban referidas al conocimiento que tiene el entrevistado respecto de la NTP de Seguridad de la Información y además busca conocer la opinión del entrevistado respecto del papel

que cumple la ONGEI en la implementación de esta norma, teniendo en cuenta el importante rol de la referida entidad en la ejecución del SGSI.

En el caso de la Dimensión Institucional, las preguntas estaban referidas a encontrar los factores, problemas y facilidades que han encontrado los oficiales de seguridad durante la implementación del SGSI en las instituciones del sector público desempeñadas. Es en esta dimensión donde se analizan a fondo los factores que dichos profesionales han ido encontrando durante la ejecución de la NTP 27001.

4.1.4. Documentación de la Entidad Pública a entrevistar

Durante el desarrollo de las entrevistas es recomendable documentarse sobre los avances que haya tenido el entrevistado respecto del tema de investigación, en la entidad pública a la cual representa. Una buena documentación nos permite tener un panorama más amplio durante la entrevista y no seamos manipulados o repetitivos, lo cual podría suceder si no estamos bien informados. Incluso, el entrevistado adquiere una mayor compenetración en la reunión, al saber que el investigador está documentado en cuanto al trabajo realizado en su organización.

Una problemática recurrente en los entrevistados se ha dado respecto del tiempo que disponen los mismos, debido a que el cargo de oficial de seguridad de la información que desempeñan es de mucha responsabilidad institucional y normalmente las entrevistas tuvieron que realizarse durante horas de descanso o al término de sus labores diarias mayormente en cafés y restaurantes cercanos al ámbito de trabajo de los entrevistados.

4.1.5. Software de transcripción de entrevistas

Mientras se realizaba la etapa de recolección de datos, se ha ido llevando a cabo -casi en paralelo- el análisis de los datos y la organización de la información. El trabajo de análisis de la información comenzó con la transcripción de las entrevistas grabadas, con las preguntas del investigador por un lado y las respuestas de los entrevistados por el otro.

En el mercado existe una diversidad de software de transcripción de entrevistas de voz a texto, cada una con diversas funcionalidades y características. Entre ellas, podemos nombrar las siguientes: Transcriber, Dragon Dictation y TalkTyper. Finalmente, se decidió trabajar con el programa ***Express Scribe***, el cual puede reproducir el audio "como si te estuvieran dictando". Por medio de esta aplicación, se podrán realizar transcripciones de toda clase de grabaciones de audio sin necesidad de detener y reanudar una y otra vez la reproducción. Además, dispone de una opción para ajustar la velocidad de la reproducción y otras opciones interesantes como el control multicanal, la gestión de ficheros y la posibilidad de usarlo con un pedal, dándole a los pies el control de la reproducción y dejando las manos libres para escribir, entre otras funcionalidades. Es importante aclarar que, a pesar de la promoción que se realiza, no existe aún un buen programa de transcripción de audio a texto directamente sin tener que transcribirlo manualmente. Estas entrevistas han sido vinculadas en los ***Anexos de Transcripciones de las Entrevistas*** (Anexos 08 al 14).

4.2. Análisis de datos de la investigación

Considerando que la investigación fue cualitativa, el análisis de datos se realizó paralelamente con la recolección de datos aplicando la metodología de la Teoría Fundamentada, donde a través del método comparativo constante el investigador simultáneamente codifica y analiza datos para desarrollar conceptos.

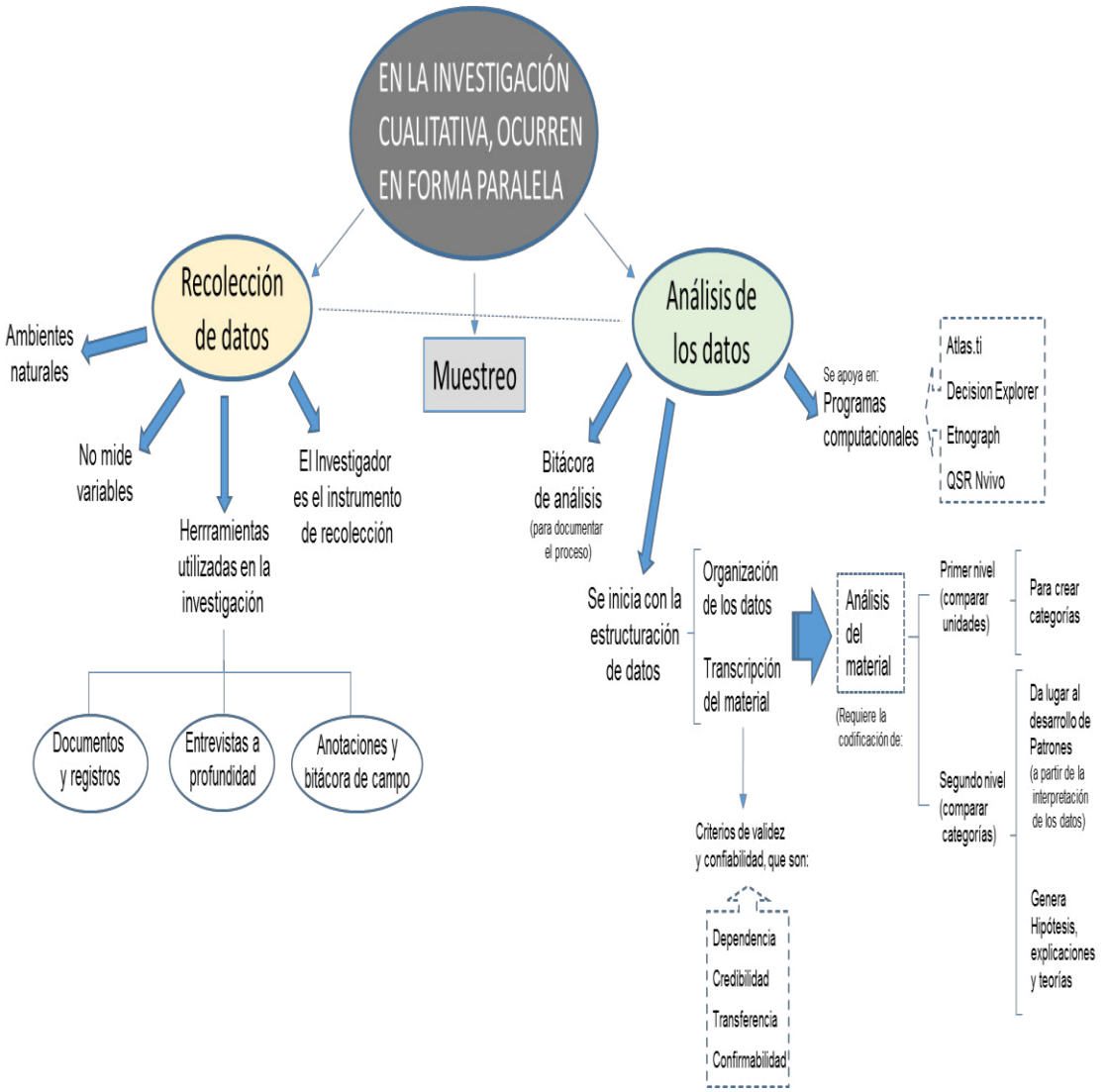


Gráfico N° 12 - **Representación del proceso de investigación cualitativa**
Fuente: **Metodología de la Investigación (2010)-Hernández Sampieri-Fernández-Baptista**

La inmersión inicial se realizó revisando la documentación pública de las instituciones definidas en la muestra y de la implementación de la NTP-ISO/IEC 27001 de los que son responsables. Luego de ello, se efectuó un análisis preliminar de la implementación de la NTP-ISO/IEC 27001, con la finalidad de identificar su nivel de importancia, las relaciones de dependencia entre ellos, el impacto individual y en conjunto para el desarrollo del gobierno electrónico.

Al momento de realizar las entrevistas en profundidad, se utilizó el proceso reflexivo con la finalidad de ir enfocando de mejor manera la entrevista y encontrar información más completa para el propósito de la investigación.

4.2.1. Organización y categorización de los datos

El análisis de datos utilizado en la investigación se efectuó utilizando el esquema de la Teoría Fundamentada, la cual consta de tres (03) etapas o fases:

1) En la primera etapa se realizó una categorización de primer nivel, en donde se codificaron las unidades de análisis en categorías. En la teoría fundamentada, este primer nivel de codificación se le denomina de ***"codificación abierta"***.

Estos códigos no mantienen relaciones de dependencia entre sí, y se presentan todos a un mismo nivel. Por tanto, se fueron identificando segmentos de texto que son importantes o significativos para el problema de investigación y se los codificó con una etiqueta representativa. Este proceso se realizó en cada uno de las entrevistas realizadas.

La recolección de datos en relación a las preguntas realizadas, implicaron además de la identificación de experiencias o conceptos en segmentos de datos (unidades), tomar decisiones respecto de qué piezas "se ajustan" entre sí para ser

categorizadas, codificadas, clasificadas y agrupadas para conformar los patrones que serán empleados con el fin de interpretar los datos (Hernández et al., 2010).

2) En una segunda etapa, se compararon las categorías entre sí, identificando diferencias y similitudes entre ellas y considerando vínculos posibles entre estas categorías. La meta era integrar dichas categorías en temas (en una categoría más general). En la teoría fundamentada, este segundo nivel de codificación se le denomina ***"codificación axial"***. A través de la codificación en estas dos fases, los códigos continúan reduciéndose hasta llegar a los elementos centrales del análisis, permitiendo conceptualizar los factores que afectan a la implementación de la seguridad de la información en las entidades públicas.

Esta *codificación axial* concluyó con el esbozo de un diagrama o modelo llamado "paradigma codificado" que muestra las relaciones entre todos los elementos.

3) En la tercera etapa, una vez generado el esquema, se regresa a las unidades o segmentos (e.g. entrevistas) y se compara con el esquema emergente para evitar abstracciones arbitrarias y poder fundamentarlo. En la teoría fundamentada, este tercer nivel de codificación se le denomina ***"codificación selectiva"***.

De ésta comparación surgieron hipótesis (las propuestas teóricas) que establecen las relaciones entre categorías o temas. Al final, se escribió un texto narrativo que vincula las categorías y describió el proceso o fenómeno.

4.2.2. Transcripción de las entrevistas

Según los datos obtenidos en las entrevistas en profundidad, se han realizado actividades de preparación para el análisis como la organización de los datos y la transcripción de las entrevistas, así como la instalación de una herramienta

informática (*softwar*e) para el análisis cualitativos de datos, el cual cumplió un papel facilitador en el análisis pero que, de ninguna manera, sustituirá el análisis creativo y profundo del investigador.

Después de averiguar todas las opciones de herramientas informáticas para el análisis cualitativo de datos, se identificó como las más usadas las siguientes: Atlas.TI, QSR Nvivo, Etnograph y Decisión Explorer.

Los criterios para seleccionar una de estas herramientas informáticas fueron las siguientes:

- Que permita realizar análisis cualitativo bajo la metodología de la teoría fundamentada,
- Que cuente con suficiente información disponible en internet,
- Que permita descargar versiones beta para analizar las herramientas;

Por tanto, luego de considerar los criterios de selección descritos en el párrafo anterior y de revisar la documentación especializada, la herramienta seleccionada para el análisis cualitativo de datos de la presente investigación fue el **ATLAS.TI**, debido a que es un software que soporta todo el proceso de la teoría fundamentada de forma eficaz y con bastante flexibilidad. **[32].**

4.3. Resultados obtenidos en las entrevistas

El procedimiento utilizado en esta investigación es de la teoría fundamentada, cuyo método es de la comparación constante, a través de una continua revisión y comparación de los datos categorizados, y que tiene como finalidad explicar la realidad basada en la recolección de los datos e interpretación de la misma, que permitirá construir hipótesis y teorías que expliquen el problema de investigación.

En esta investigación, el problema de estudio responde a la siguiente pregunta: ***¿Qué factores son los que afectan la implementación del Sistema de Gestión de Seguridad de la Información -SGSI- en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001?***

En la presente investigación cualitativa, se han realizado entrevistas a profundidad a los Oficiales de Seguridad de la Información encargados de la implementación del SGSI en sus respectivas instituciones públicas de acuerdo a la NTP-ISO/IEC 27001.

Cada una de las entrevistas ha sido oficializada adjuntando el formato de consentimiento informado por parte del entrevistador y la transcripción de cada entrevista. En los Anexos 8 al 13 se detalla la transcripción de cada una de ellas.

4.3.1. Análisis de datos de la primera entrevista

Luego del ***análisis de datos realizado en la primera entrevista***, se han encontrado los siguientes factores que afectan la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la institución.

Respecto de las restricciones en las políticas de gobierno, la percepción que se tiene del desempeño de la ONGEI es insuficiente, ya que si bien es el ente normativo de informática en el Estado Peruano no es una entidad netamente autónoma debido a ciertas limitaciones principalmente funcionales. Asimismo, la ONGEI se ve afectada por los constantes cambios organizacionales lo que perjudica su labor consultiva. Finalmente, se infiere de la entrevista que el oficial de seguridad de la información no está formalizado en la estructura funcional institucional y, al no estar en los

instrumentos de gestión institucional como son el ROF y MOF, no cuentan con un cargo y un presupuesto designados.

Respecto de las restricciones en la parte operativa:

- En relación a la gestión, se ha determinado que existe un desconocimiento respecto de su operatividad. En esta institución, el personal de desarrollo tenía un concepto de que para implementar el SGSI, primero tenía que tener el inventario de todos los activos de información, luego la infraestructura y finalmente tener el personal idóneo. Asimismo, se pensaba que sin el software no se podía realizar su ejecución.

  Actualmente, como parte de los procesos de implementación del SGSI lo que se está utilizando es un órgano de apoyo de la institución. En este caso, se está tomando como un estándar el centro de datos o los sistemas de información cuando normalmente el SGSI deber reposar en un proceso core del negocio el cual se encuentra generalmente en las áreas estratégicas o funcionales.
- En relación al apoyo institucional, no existe el respaldo necesario para que se desarrolle esta NTP pero no porque no se quiera sino porque no han sido concientizados de la mejor forma. Es decir, no se tiene un conocimiento de la magnitud del problema que se puede generar al no implementar este sistema de gestión en la institución, así como los constantes cambios de gestión que suceden a menudo.
- En relación a la normatividad, si bien las referencias normativas son claras, la norma debe ser adecuada a la necesidad de la organización para que se tome explícitamente lo que se necesita en la entidad.
- En referencia a la organización del SGSI, no se tiene definido un alcance estandarizado institucional, se tienen los procesos macro pero no se tienen los

procesos específicos, no están con sus diagramas de flujos ni sus procedimientos. Es importante que se tenga un buen conocimiento de procesos para poder definir cómo un proceso se interrelaciona con otro, lo que finalmente determinará el Alcance del SGSI. Sin embargo, en las instituciones públicas el determinar un proceso implica tener que reunirse con las áreas involucradas lo que conlleva a problemas de coordinación. Por tanto, debería existir un área de procesos que le ayude al oficial de seguridad de información a determinar cuál es el mejor proceso de la organización para iniciar el SGSI.

Respecto de las restricciones de desarrollo de la NTP, si bien los objetivos en la institución, tales como la implementación de mecanismos de seguridad de la información y la aplicación de una metodología más eficaz en SGSI están claramente definidos, la implementación está más enfocada a temas de seguridad en sistemas de información o sistemas de comunicación de datos.

Respecto del presupuesto, las entidades no han tenido un conocimiento exacto de cómo implementar presupuestalmente la NTP debido a que por ejemplo cogían esta norma como sustento técnico para los pedidos de compras de equipos de seguridad pero en forma aislada no relacionándolas más adelante con los permisos o contraseñas al personal de la institución.

Respecto de la especialización, el cargo de oficial de seguridad de información recae en un personal sin experiencia. En la mayoría de los casos este cargo lo asume el Jefe o algún personal de TI, los mismos que por tener funciones ya asignadas por el cargo que desempeñan, se les hace difícil realizar las actividades concernientes a la implementación del SGSI. En dicho cargo se necesita personal con experiencia con la capacitación necesaria, a fin de que sea el interlocutor entre la Alta Dirección

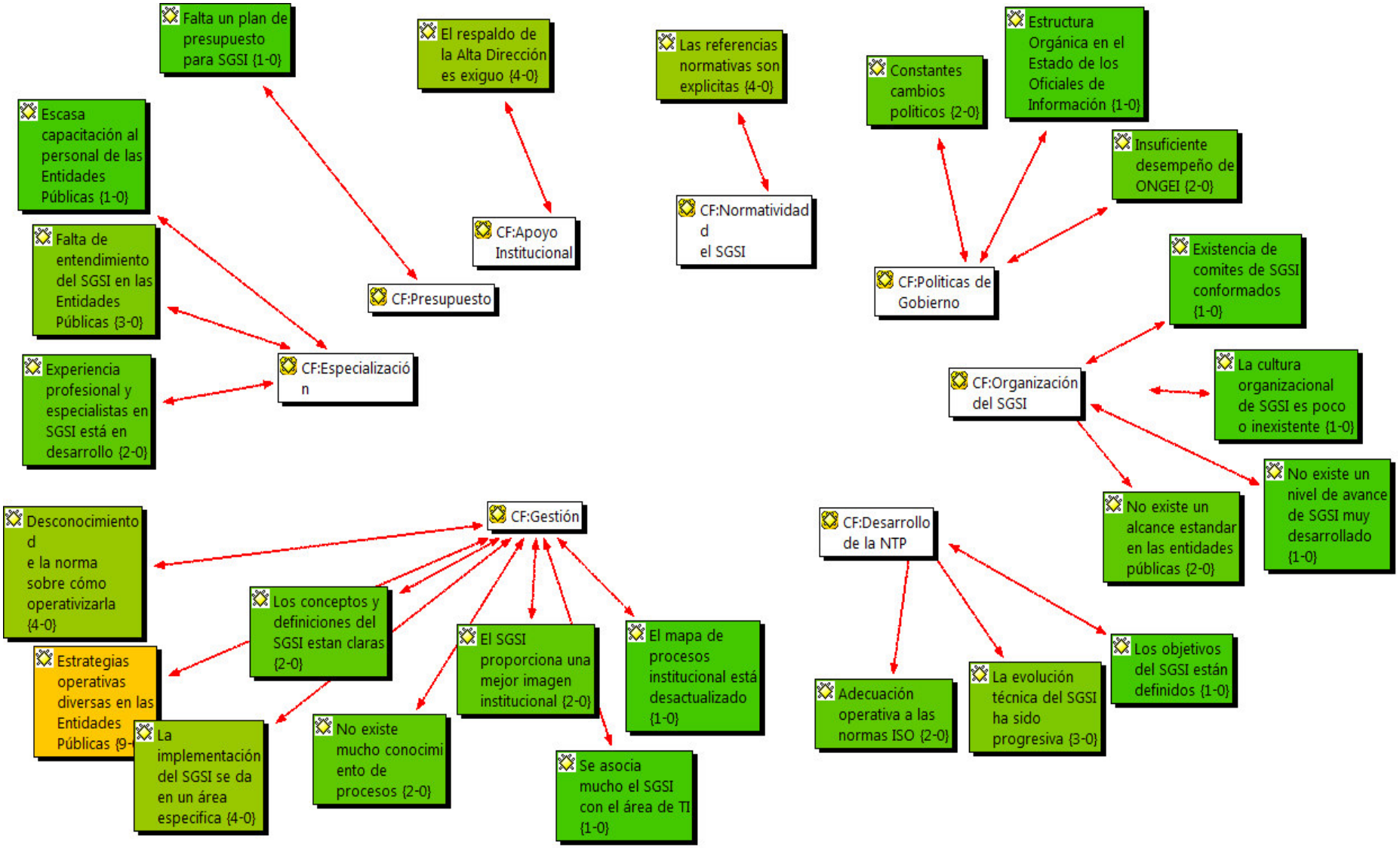
y las demás dependencias de la institución y además que esté a tiempo completo para realizar la implementación del SGSI.

En el siguiente cuadro podemos visualizar un resumen de los factores y sus indicadores encontrados en la primera entrevista:

Factores que afectan la implementación del SGSI en las entidades públicas	Indicadores encontrados en la 1ra. Entrevista	N° incid.
1. Políticas de Gobierno	1.1. Insuficiente desempeño de la ONGEI	1
	1.2. Constantes cambios políticos en el Estado	1
	1.4. Estructura orgánica y funcional del Oficial de Seguridad en las Entidades del Estado	1
2. Desarrollo de la NTP	2.1. Los objetivos están definidos	1
	2.2. Evolución técnica progresiva	1
	2.3. Falta de adecuación operativa a las norma standard ISO	1
3. Presupuesto	3.1. Falta un plan de presupuesto para SGSI.	1
4. Especialización	4.1. Escasa capacitación el personal de las entidades públicas.	1
	4.3. La experiencia profesional en SGSI aún está en desarrollo	1
5. Gestión del SGSI	5.2. Existe desconocimiento respecto de su operatividad	2
	5.4. Estrategias Operativas diversas en las instituciones	2
	5.5. El SGSI proporciona una mayor imagen institucional	1
	5.8. Se asocia mucho SGSI con el área de TI (creencia que TI es el que debe implementarlo)	1
	5.9. No existe mucho conocimiento de procesos	1
6. Apoyo Institucional	6.1. El respaldo de la Alta Dirección es exiguo (x desconocer importancia)	4
8. Organización del SGSI	8.1. No se define un alcance estandarizado en las instituciones (generalmente DC)	3
	8.4. La cultura organizacional del SGSI es poca o inexistente	1

Tabla N° 5: **Identificación de los indicadores encontrados en la Primera Entrevista en cada uno de los factores formulados**

Gráfico N° 13: **Diagrama de Análisis de Datos de la Primera Entrevista**



4.3.2. Análisis de datos de la segunda entrevista

Luego del ***análisis de datos realizado en la segunda entrevista***, se han encontrado los siguientes factores que afectan la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la institución.

Respecto de las restricciones en las políticas de gobierno, se considera que la ONGEI ha cumplido su papel de ente rector en la implementación del SGSI hasta cierto punto pero sigue siendo insuficiente faltándole mejorar muchas cosas aún. Se recomienda, la existencia de un set de profesionales consultores que le den soporte a todas las instituciones públicas.

Asimismo, si bien es cierto que la seguridad de la información es un tema prioritario para nuestro país, no hay el apoyo político a nivel de Estado. Debería existir como política de gobierno. Es necesario desarrollar un plan de seguridad que permita implementar, verificar y controlar estos sistemas pero no a nivel institucional sino a nivel de país y que permitan optimizar el uso de los recursos a través de una política clara que permita manejar y unificar esfuerzos interinstitucionales. *"Así como se tienen otros objetivos de país sobre la pobreza o sobre el desarrollo económico, debería haber un objetivo similar en lo que respecta a cuidar y proteger nuestra información como Estado y que mejor en nuestras instituciones públicas".*

Este plan debe ser desarrollado a través de un conjunto de lineamientos integrales, como son: Primero, el control interno debe estar bien implantado en las organizaciones. Segundo, la continuidad de negocios tiene que estar relacionado con la seguridad de información. Ambos tienen que conversar. Un tercer elemento es el Gobierno de las Tecnologías de la Información y las Comunicaciones que también deberán estar

relacionados a los dos anteriores. Es decir, que son varios frentes de una organización que tienen que trabajar de forma integrada para lograr un frente común.

Finalmente, de la entrevista se desprende que el Oficial de Seguridad no existe como un rol (en el ROF institucional) como tantos otros roles existentes en el Estado. Generalmente, este rol muchas empresas lo toman como algo momentáneo: *"mientras implementemos el ISO 27000, contratamos personal especialista y luego una vez que termine, se termina el proyecto y todos se van"*. Se concluye, por tanto, que no existe un rol de oficial de seguridad de la información institucionalizado.

Respecto de las restricciones en la parte operativa:

- En relación a la gestión, se establece que la norma de seguridad de la información ayuda a cumplir con los objetivos estratégicos que se ha trazado la institución. Dentro de estos objetivos está la de brindar servicios de calidad relacionados con la tecnología.

  Además, las estrategias operativas de implementación del SGSI en las instituciones son diversas donde unas lo tienen más desarrolladas que otras. Actualmente, las instituciones públicas se están disparando cada una por su lado, cada una busca sus consultores, cada una busca contratar una empresa que lo ayude a implementar. Todas lo hacen a su manera, pero no hay un ente que reúna a un conjunto de especialistas los cuales pueden estar a disposición del monitoreo del avance del SGSI en las entidades públicas.

  Otro factor restrictivo es que el establecimiento de procesos de muchas instituciones públicas es inexistente o han ido cambiando en el tiempo están desactualizadas. No sucede así con esta institución que es una de las pocas que se

ha certificado en SGSI en un proceso, teniendo 04 procesos claves más en desarrollo. Por ello, se termina haciendo una acotación de que no necesariamente una entidad que está certificada se podría decir que está implementada al 100%.

Hay que destacar que en esta organización, la oficina de seguridad de la información está en otra área diferente al área de TI, el cual es un órgano a nivel de asesoría y que reporta directamente a la alta dirección. Se recomienda que, en el caso de las entidades públicas, los oficiales de seguridad de la información no deban pertenecer a las áreas de TI porque de alguna forma se convierten en juez y parte, y eso es lo que se debe evitar.

- En relación al apoyo institucional, existe el respaldo total de la Alta Dirección y le dan la importancia debida, tanto así que ahora se encuentran implementándolo en 02 procesos más. Sin embargo, existe aún una falta de cultura del SGSI de la Alta Dirección, ya que muchas instituciones piensan que cuando hablamos de seguridad de la información estamos hablando de tecnología solamente.
- En relación a la normatividad, se tiene bien en claro que el objetivo principal es proteger la información del Estado. Con esta norma, nuestro país está en línea a las normas internacionales que salvaguarda la información y que es considerada actualmente como el activo más importante de una organización.
- En relación a la organización del SGSI, la normativa de la NTP no precisa claramente el Alcance que deben definir las organizaciones. Por tanto, en el Alcance se puede especificar un área, un proceso, un sub-proceso o toda la institución y eso es justamente quizás uno de los errores más comunes que se está manejando. Tiene que haber un estudio preliminar para poder determinar el alcance real y que esto se alinee a los objetivos estratégicos que busca la Organización.

En esta organización, se tiene conformado un Comité de Gestión de Seguridad de la Información que está integrado por los entes máximos de la Institución, un oficial de seguridad y, algo que destacar aquí es la existencia de coordinadores de seguridad de la información en cada área de la Institución.

Esto tiene que ver con la aplicación de una estrategia de implementación descentralizada y no de forma centralizada: De forma centralizada es cuando se pone un oficial de seguridad y un pool de analistas que verán la seguridad de la información de toda la institución. Mientras que en la descentralizada, se tiene un oficial de seguridad y coordinadores de seguridad en cada una de las áreas de la organización, por más chica que sean estas. Estos coordinadores, en algunos casos y dependiendo de la complejidad del proceso, están dedicados a full- time y en otros casos a medio tiempo. Asimismo, deben cumplir con un perfil mínimo de especialidad en seguridad de información, los cuales además de tener funciones específicas tendrán una capacitación y posterior evaluación. Todo esto es parte de un proceso de aprendizaje continuo.

Los programas de capacitación en SGSI están dirigidos a diferentes segmentos: Existen capacitaciones dirigidas a la Alta Dirección, capacitaciones dirigidas a los Coordinadores de seguridad de la información y capacitaciones dirigidas a todo el personal de la institución. Este proceso de inducción es una especie de nivel de madurez, *"es un proceso de evangelización"*.

Respecto de las restricciones de desarrollo de la NTP, es de destacar la experiencia obtenida en el desarrollo de procesos basados en la ISO 9000. Esto ha permitido administrar una cultura sobre los sistemas de gestión.

La ventaja de ello es que muchos de los documentos del sistema de gestión de la ISO 9001, son comunes para la ISO 27001 y eso ayuda mucho. Estos documentos comunes, en algunos casos varían, en lo mínimo, pero cumplen el mismo rol.

Respecto del presupuesto, es importante tener en cuenta que muchas instituciones públicas o no tienen el presupuesto necesario o no lo han sustentado debidamente, y por tanto, les resulta difícil implementarlo. Sin embargo, en otras instituciones a pesar de contar con el presupuesto necesario, todavía existen dificultades respecto del cargo de oficial de seguridad de la información, el cual al ser bastante especializado y muy técnico, son las gerencias de RR.HH. que todavía no tienen bien claro dicha funcionalidad y piensan que el rol de oficial de seguridad de información lo puede asumir cualquier persona o es un trabajo técnico.

Por otro lado, debe tenerse presente que la implementación de un sistema de gestión, no es solamente el costo de implementación del proyecto, sino que hay que contemplar dicha implementación más el costo del mantenimiento y esto incluye poner un equipo de personas nuevo en la entidad: un oficial de seguridad, un analista de seguridad, y que estos formen parte permanente de la institución para su mantenimiento y actualización.

Respecto de la especialización, un factor altamente restrictivo es la alta rotación del personal de las instituciones públicas donde muy poca es la que está en planilla. Generalmente casi todos son contratados como CAS o servicio de terceros. Entonces, no hay una continuidad del personal y, en muchos de los casos, este personal está pensando en su bienestar económico más que en el de la institución y del país. Otro factor también que influye es el de los sueldos en la institución

pública y que varían demasiado con respecto a los de las privadas. Por ello, es muy difícil que un buen profesional quiera trabajar en una institución pública.

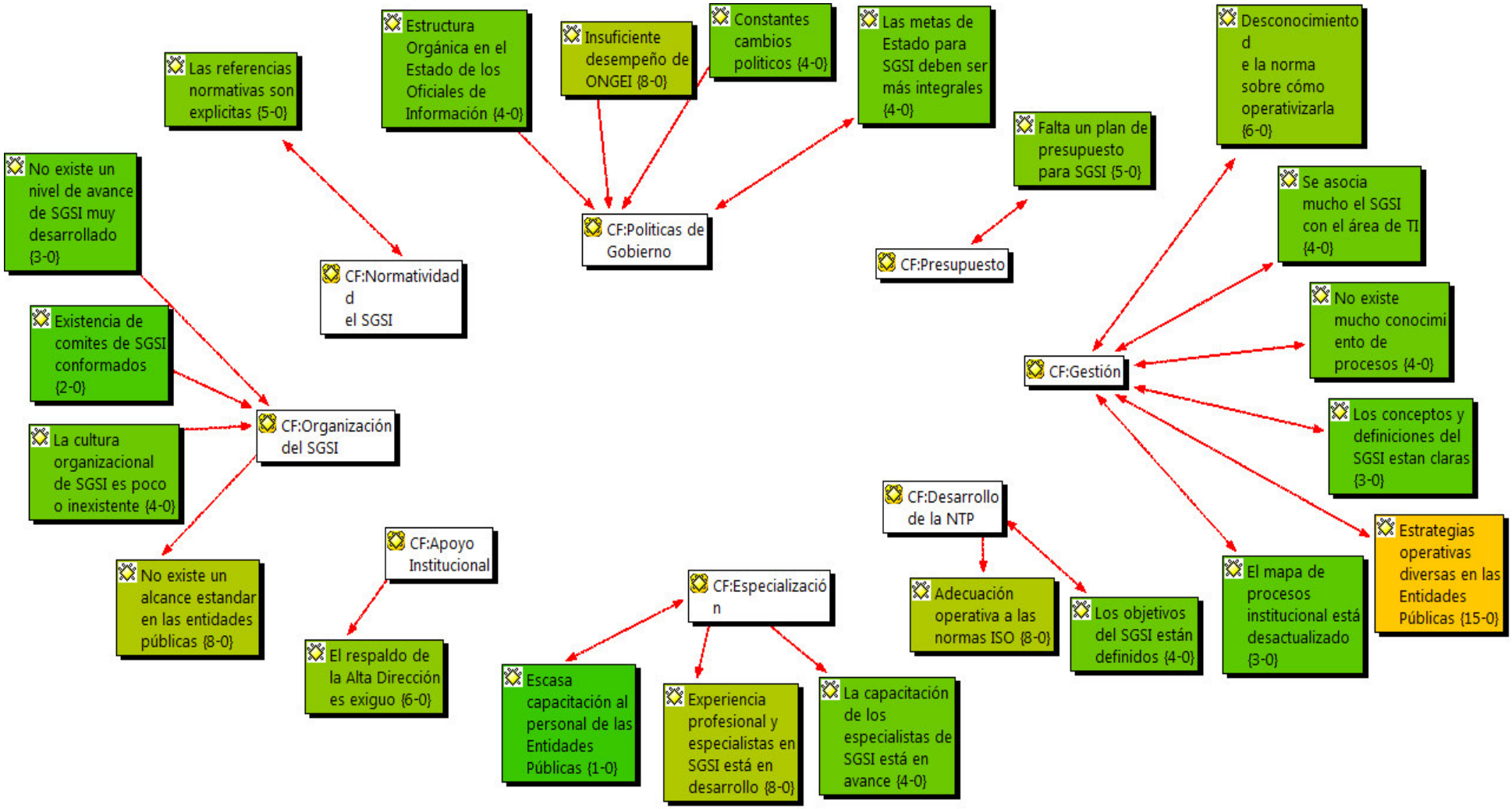
Finalmente, la falta de profesionales especializados en la implementación del SGSI es muy escaso en nuestro país. Por tanto, es necesario que se pueda contar con un staff de especialistas peruanos y extranjeros con conocimiento en este tema.

En el siguiente cuadro podemos visualizar un resumen de los factores y sus indicadores encontrados en la segunda entrevista:

Factores que afectan la implementación del SGSI en las entidades públicas	Indicadores encontrados en la 2da. Entrevista	N° incid.
1. Políticas de Gobierno	1.1. Insuficiente desempeño de la ONGEI	1
	1.2. Constantes cambios políticos en el Estado	1
	1.3. Metas de Estado para el SGSI deben ser más integrales	3
	1.4. Estructura orgánica y funcional del Oficial de Seguridad en las Entidades del Estado	1
2. Desarrollo de la NTP	2.3. Falta de adecuación operativa a las norma standard ISO	2
3. Presupuesto	3.1. Falta un plan de presupuesto para SGSI	3
4. Especialización	4.3. La experiencia profesional en SGSI aún está en desarrollo	3
5. Gestión del SGSI	5.3. Los conceptos y definiciones del SGSI están claros	2
	5.4. Estrategias Operativas diversas en las instituciones	3
	5.6. El mapa de procesos institucional está desactualizado	4
	5.8. Se asocia mucho SGSI con el área de TI (creencia que TI debe implementar)	2
6. Apoyo Institucional	6.1. El respaldo de la Alta Dirección es exiguo (x desconocer importancia)	5
7. Normatividad del SGSI	7.1. No existe un entendimiento normativo claro de la norma	1
8. Organización del SGSI	8.1. No se define un alcance estandarizado en las instituciones (gralm. es el DC)	3
	8.2. Ya existen comités de SGSI conformados	2
	8.3. No existe un nivel de avance del SGSI muy desarrollado en las instituciones	4
	8.4. La cultura organizacional del SGSI es poca o inexistente	1

Tabla N° 6: **Identificación de los indicadores encontrados en la Segunda Entrevista en cada uno de los factores formulados**

Gráfico N° 14: **Diagrama de Análisis de Datos de la Segunda Entrevista**



4.3.3. Análisis de datos de la tercera entrevista

Luego del ***análisis de datos realizado en la tercera entrevista***, se han encontrado los siguientes factores que afectan la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la institución.

Respecto de las restricciones en las políticas de gobierno, se tiene presente la existencia de un equipo de trabajo en ONGEI referente a la seguridad de la información que reúne a las entidades públicas mensualmente pero se considera que no es suficiente. Se recomienda que debiera existir una normatividad quincenal o mensual que requiera la verificación de los avances realizados y los problemas encontrados, lo cual no existe actualmente.

La apreciación que se tiene de la ONGEI es que si bien es un órgano rector o coordinador, no lo realiza como debería ser ya que tendría que cumplir un rol más activo, pasar a ser una entidad más proactiva. Este problema, se presenta principalmente a los diferentes cambios estructurales que se suceden en ONGEI. Esta dificultad también se presenta entre las instituciones obligadas a la implementación de la NTP, donde pueden cambiar sus prioridades y apoyo directivo en cualquier momento.

Por otro lado, las instituciones vienen realizando la implementación más bien por la presión de la Contraloría, ya que ellos son los que observan los avances realizados sobre el SGSI entre otros aspectos. Por tanto, se actúa más en la implementación del SGSI por la fiscalización de la Contraloría que por el trabajo de la ONGEI.

Todo esto nos conlleva a pensar en que la ONGEI debe asumir un rol más proactivo, estableciendo una agenda de reuniones periódicas (quincenales o mensuales). Tiene que

asumir un mayor liderazgo. *"Actualmente, cada institución del Estado camina a su manera de la mejor forma que puede"*.

Una de las propuestas podría ser por ejemplo, reunir a un grupo de entidades para intercambiar ideas y experiencias en el avance de la implementación del SGSI en las instituciones públicas. Se podrían incluso hacer convenios interinstitucionales ya que la ley me permite hacer ello: *"A veces nos falta un poco más de unión como Estado, cada entidad como que trabaja en lo suyo, no se comparten aprendizajes"*.

Finalmente, un factor esencial que se presenta al implementar la NTP es que no está normado el cargo de oficial de seguridad en el ROF y MOF del Estado Peruano. Actualmente, los oficiales de seguridad no existen en el mapa estatal. Este es un trabajo pendiente de ONGEI que le atañe directamente y que además debería establecerse que este cargo no dependa del área de informática sino de la Alta Dirección.

Respecto de las restricciones en la parte operativa:

- En relación a la gestión, existe un problema que se percibe respecto de las diferentes normas que se van actualizando. Actualmente se tiene cierto desconocimiento de la norma actual sobre cómo operativizarla. *"Pienso que la norma 17799 tuvo más impacto que la 27001, ya que se podía mirar el procedimiento, se atacaba algo puntual"*.

  Por otro lado, las instituciones manejan diversas estrategias operativas, en nuestro caso por ejemplo, la parte técnica la verá el oficial de seguridad con un equipo de consultores que se ha contratado, dejando la parte administrativa al comité de trabajo de la institución.

Otro factor problemático muy importante es que los procesos no están debidamente formalizados. Según el entrevistado, los únicos procesos que están medianamente establecidos con directivas son los procesos administrativos. Se recomienda realizar un mapa de procesos de la institución.

Otro problema que se presenta en las instituciones es que normalmente le encargan la implementación del SGSI al área de informática. No obstante, el jefe de informática lo podría liderar, por su misma formación, podría confundir lo que es seguridad informática con seguridad de información. Además, el oficial de seguridad debería depender directamente de la Alta Dirección porque él tiene un rol más amplio que el jefe de informática, uno es operativo pero el otro es de supervisión. Por tanto, el oficial de seguridad no debería ser el jefe de informática.

- En relación al apoyo institucional, se considera que el apoyo de la Alta Dirección es parcial, no es total. Es el jefe mismo de la institución el que se involucre, aporte y retransmita a todos sus subordinados la importancia de implementar el SGSI. Sin embargo, no todos en la Alta Dirección lo tienen claro. Por ello, sería necesario brindarles un curso de concienciación a todos los directores y allí explicarles bien la importancia del mismo.
- En relación a la normatividad, tal como se comentó en la gestión del SGSI, la norma NTP 17799, que estaba enfocada a los procedimientos y controles en sí, no a todo el sistema de gestión y allí se implementaban ciertas políticas de seguridad de la información. Sin embargo, la norma NTP 27001 te cambia la figura, ya que la anterior estaba orientada a la parte operativa y no a la gestión.

Desde un inicio debió ser en la parte de gestión primero y luego en la parte operativa. La norma actual rectifica este problema.

- En relación a la organización del SGSI, no se tiene un Alcance del SGSI estandarizado. En la mayoría de las instituciones es el Centro de Datos del área de informática la que se toma como parámetro. Asimismo, se suele poner al oficial de seguridad como la persona que lidera el comité de seguridad de la información en la institución.

Respecto de las restricciones de desarrollo de la NTP, se ha encontrado más bien un aspecto positivo en el ordenamiento y clasificación de la información que se brinda al ciudadano. La Alta Dirección ha comprendido la importancia del SGSI y el papel del oficial de seguridad de información en relación a qué tipo de información se brinda ante el requerimiento de alguna solicitud externa específica.

Respecto del presupuesto, este es un factor **que** está ligado a la politización de la Alta Dirección respecto del apoyo que le den a esta norma. Este apoyo depende mucho del compromiso que tengan las autoridades principales de turno y esto se verá reflejado en el presupuesto asignado para la implementación del SGSI.

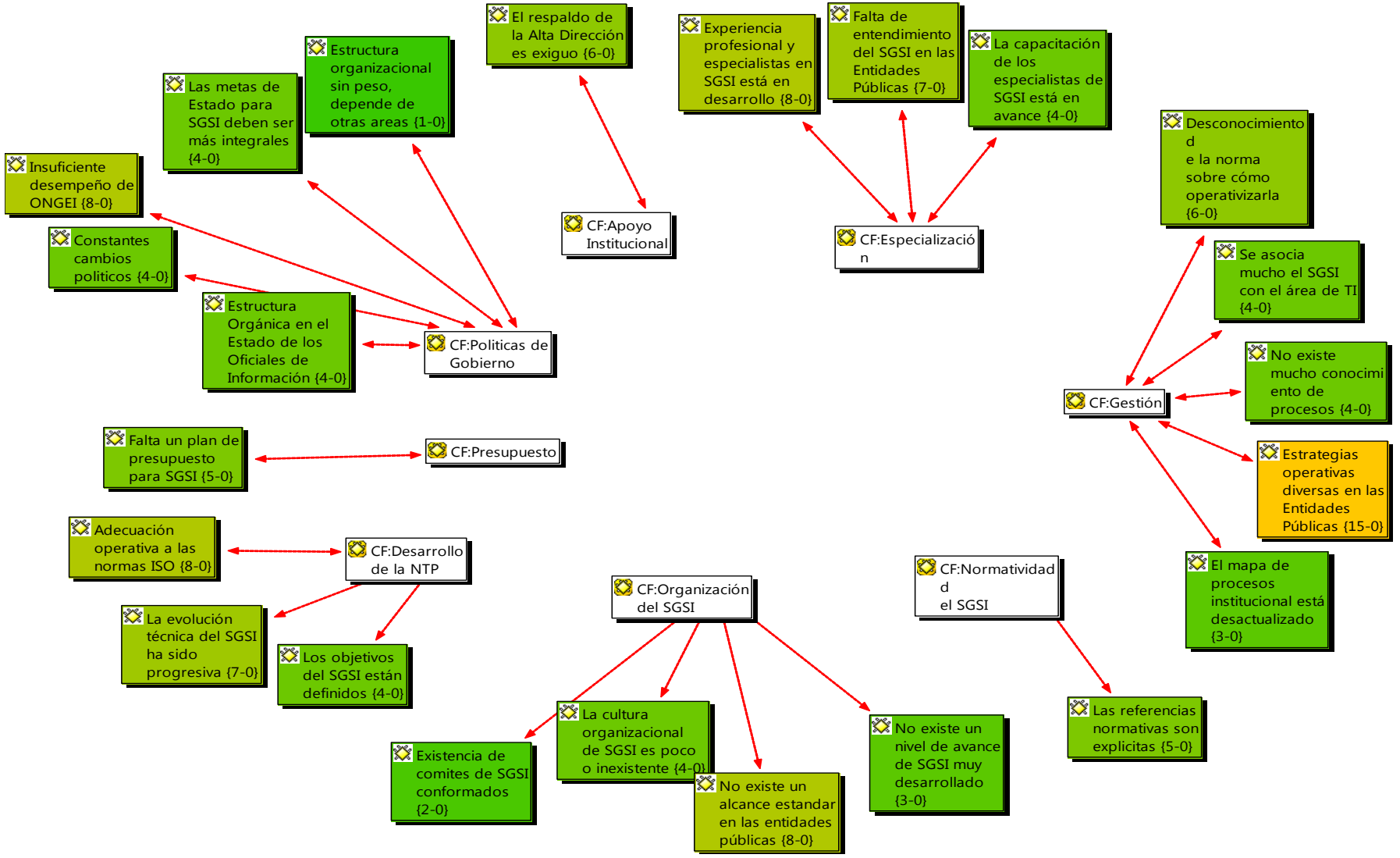
Respecto de la especialización, se ha manifestado que no hay personal capacitado eficientemente en el Estado para implementar esta norma, *"la mayoría estamos en proceso de aprendizaje".* Por otro lado, la mayoría de los oficiales de seguridad de información que asisten a las reuniones de la ONGEI son los jefes de informática de las entidades públicas.

En el siguiente cuadro podemos visualizar un resumen de los factores y sus indicadores encontrados en la tercera entrevista:

Factores que afectan la implementación del SGSI en las entidades públicas	Indicadores encontrados en la 3ra. Entrevista	N° indic.
1. Políticas de Gobierno	1.1. Insuficiente desempeño de la ONGEI	2
	1.2. Constantes cambios políticos en el Estado	2
	1.3. Metas de Estado para SGSI	4
	1.4. Estructura orgánica y funcional del Oficial de Seguridad en las Entidades del Estado	2
2. Desarrollo de la NTP	2.1. Los objetivos están definidos	2
	2.3. Falta de adecuación operativa a las norma standard ISO	1
3. Presupuesto	3.1. Falta un plan de presupuesto para SGSI.	2
4. Especialización	4.3. La experiencia profesional en SGSI aún está en desarrollo	1
	4.4. La capacitación profesional de especialistas en SGSI está avanzando	1
5. Gestión del SGSI	5.2. Existe desconocimiento respecto de su operatividad	2
	5.4. Estrategias Operativas diversas en las instituciones	2
	5.6. El mapa de procesos institucional está desactualizado	2
	5.8. Se asocia mucho SGSI con el área de TI (creencia que TI debe implementar)	1
6. Apoyo Institucional	6.1. El respaldo de la Alta Dirección es exiguo (x desconocer importancia)	2
7. Normatividad del SGSI	7.1. No existe un entendimiento normativo claro de la norma	1
8. Organización del SGSI	8.1. No se define un alcance estandarizado en las instituciones (generalmente es el DC)	2
	8.2. Ya existen comités de SGSI conformados	1
	8.4. La cultura organizacional del SGSI es poca o inexistente	1

Tabla N° 7: **Identificación de los indicadores encontrados en la Tercera Entrevista en cada uno de los factores formulados**

Gráfico N° 15: **Diagrama de Análisis de Datos de la Tercera Entrevista**



4.3.4. Análisis de datos de la cuarta entrevista

Luego del ***análisis de datos realizado en la cuarta entrevista***, se han encontrado los siguientes factores que afectan la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la institución.

Respecto de las restricciones en las políticas de gobierno, se concluye que la ONGEI si bien viene cumpliendo un papel de ente normativo, no está haciendo un papel de ente implementador. Esta entidad debería tomar acciones que permitan la articulación entre las entidades, sobre todo en aquellas ya certificadas las cuales pudieran enseñar a otras entidades que aún están en la etapa de implementación. Además, se recomienda que ONGEI podría también reunir a todas las altas autoridades del Estado y brindarles una capacitación en SGSI, teniendo en cuenta que la seguridad de la información es un objetivo estratégico de una Política de Estado. Por otro lado, se reitera que el cargo de seguridad de la información no existe a nivel del ROF y MOF de la institución.

Finalmente, se remarca la importancia de tener una Política Nacional de Seguridad de la Información. *"Más que dar la norma deberíamos buscar la forma de todos conozcan la importancia de la seguridad de la información en cada una de sus instituciones"*.

Respecto de las restricciones en la parte operativa:

- En relación a la gestión, el principal problema operativo para su implementación es que las instituciones no llegan a trabajar como gobierno, es decir, todas juntas como un equipo. *"No obstante hay esfuerzos aislados de algunas instituciones, no se visualiza un esfuerzo orientado hacia una implementación en conjunto. Al menos, debería trabajarse a nivel de sectores de gobierno"*.

Ahora bien, otro factor que influye es que se piensa que la seguridad de la información está asociada netamente a informática, que es una función de TI. Muchas instituciones confunden o limitan la seguridad de la información solamente al área tecnológica y eso es un error, porque se deja de lado todas las demás áreas y el personal de ellas no se quieren involucrarse mucho porque piensan que eso una tarea de TI. Asímismo, es muy importante tener los procesos claros al implementar la seguridad de la información, sobre todo al momento de identificar los activos de información. *"Tener un proceso claro te da una visión de negocio y con eso puedes identificar bien lo que quieres implementar"*.

Hay que indicar que esta institución pública (que recordamos ha certificado en SGSI) tenemos el ISO 9000 también. Entonces, el conjunto de estos ISO´s (27000 y 9000) ha hecho que los procesos estén más ordenados. *"Actualmente, nosotros tenemos certificados 11 procesos (en 9001), y de estos no todos van a tener 27001 sino solamente aquellos en los que se requieran niveles de seguridad"*.

En este caso lo que se ha optado en esta entidad es que los procesos que requieren seguridad de la información y que ya tienen ISO 9001, son los candidatos a pasar a esta NTP 27001. Primero porque es más fácil, ya que se tiene una estructura de sistema de gestión y sobre eso se implementan los controles y todo lo referente a gestión de riesgos.

- En relación al <u>apoyo institucional</u>, la Alta Dirección tiene clara la importancia de la implementación del SGSI y está dentro de sus objetivos, esto también en parte porque el jefe nacional es un "fanático" de los sistemas de gestión. *"Pienso que es*

un factor muy importante el poder vender la seguridad de la información en las instituciones".

- En relación a la organización del SGSI, se tiene un comité de gestión y un comité operativo de seguridad de la información. En el comité de gestión se tiene a la Alta Dirección a la cabeza y está conformado por casi todos los gerentes de la entidad. El Comité Operativo con el oficial de seguridad a la cabeza, está conformado por los responsables de Seguridad de la Información de cada gerencia, los cuales no son gerentes sino especialistas, no en seguridad sino en las funciones de su gerencia. "*Por ejemplo, se cuenta con un abogado especialista en temas informático-legales, y donde el oficial de seguridad trabaja con este especialista*".

  Sin embargo, el mayor obstáculo que se presenta siempre es la de crear conciencia al personal, cambiar los hábitos de trabajo, lo cual es difícil de modificar en las personas.

Respecto de las restricciones de desarrollo de la NTP, no se tiene mayor problema en ello debido a que la implementación de la seguridad de información en la institución viene desarrollándose hace muchos años y lo que se hace es mantener ordenada la ejecución de los controles de seguridad y perfeccionarlos a través de un sistema de gestión de mejora continua.

Respecto de la especialización, se puede concluir que la seguridad de la información es un componente dentro del programa de inducción. *"En las áreas operativas, cuando hay cambios de puestos o de nuevo personal, éstas pueden solicitar capacitación en seguridad de información".*

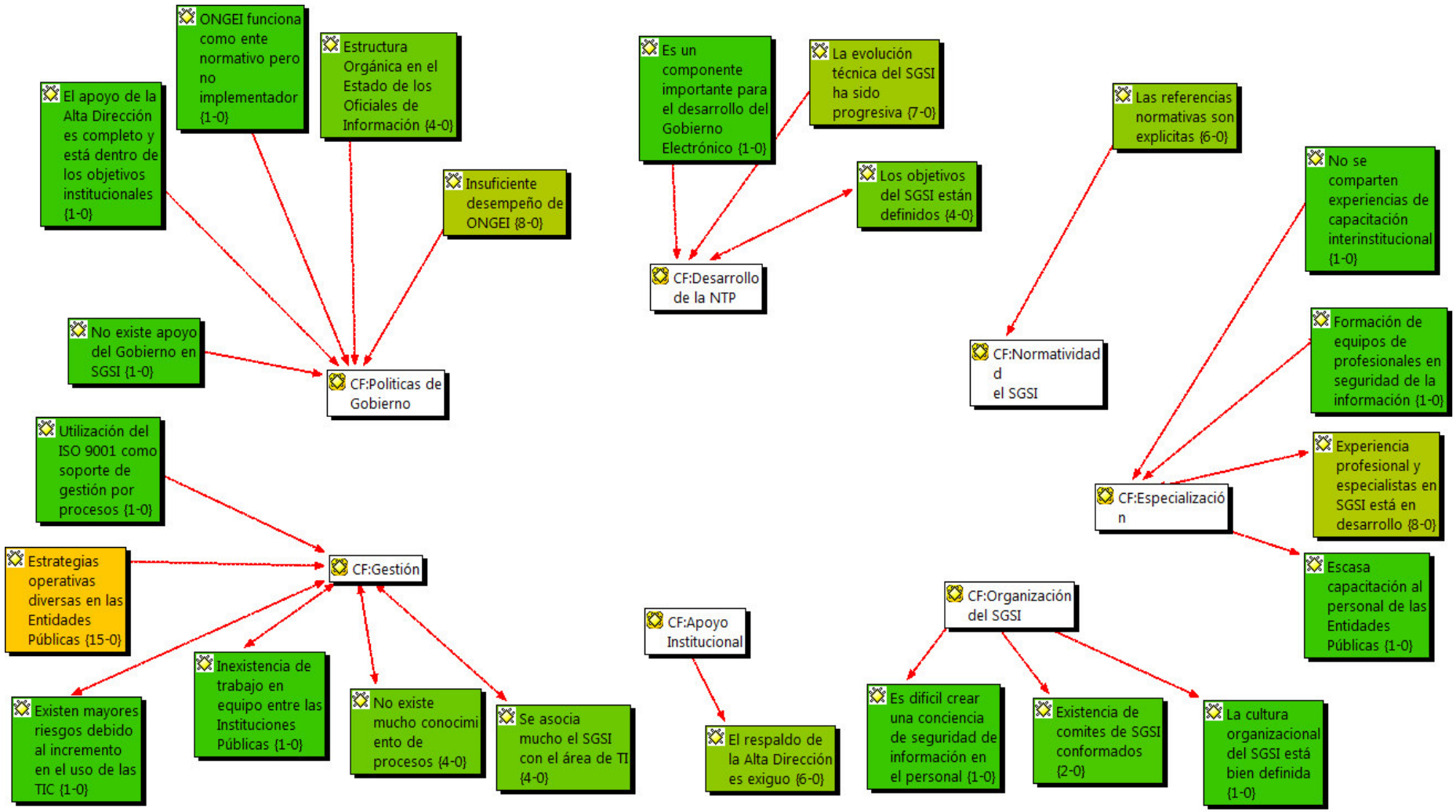
Se hace la recomendación de que el Estado debiera formar personas que pudieran realizar la labor de asesoramiento en SGSI, debido a que muchas instituciones (a veces por desconocimiento) terminan haciendo contrataciones externas para realizar implementaciones de servicios de seguridad de información que en realidad no son las más óptimas, lo cual no beneficia a la institución sino únicamente al proveedor.

En el siguiente cuadro podemos visualizar un resumen de los factores y sus indicadores encontrados en la cuarta entrevista:

Factores que afectan la implementación del SGSI en las Entidades Públicas	Indicadores encontrados en la 4ta. Entrevista	N° incid.
1. Políticas de Gobierno	1.1. Insuficiente desempeño de la ONGEI	1
	1.4. Estructura orgánica y funcional del Oficial de Seguridad en las Entidades del Estado	1
	1.5. No existe apoyo del Gobierno en SGSI	1
	1.6. ONGEI funciona como ente normativo pero no implementador	3
2. Desarrollo de la NTP	2.1. Los objetivos están definidos	1
	2.3. Adecuación operativa a las norma estándar ISO	1
4. Especialización	4.1. Escasa capacitación el personal de las entidades públicas.	1
	4.3. La experiencia profesional y de especialistas en SGSI aún está en desarrollo	1
	4.5. Formación de equipos de profesionales en seguridad de la información	1
5. Gestión del SGSI	5.4. Estrategias Operativas diversas en las instituciones	3
	5.8. Se asocia mucho SGSI con el área de TI (creencia que TI debe implementar)	3
	5.9. No existe mucho conocimiento de procesos	2
	5.10. Existen mayores riesgos debido al incremento en el uso de las TIC	1
	5.11. Utilización del ISO 9001 como soporte de gestión por procesos	3
6. Apoyo Institucional	6.1. El respaldo de la Alta Dirección es exiguo (x desconocer importancia)	2
8. Organización del SGSI	8.1. No se define un alcance estandarizado en las instituciones (generalmente es el DC)	1
	8.2. Ya existen comités de SGSI conformados	2
	8.4. La cultura organizacional del SGSI es poca o inexistente	1

Tabla N° 8: **Identificación de los indicadores encontrados en la Cuarta Entrevista en cada uno de los factores formulados**

Gráfico N° 16: **Diagrama de Análisis de Datos de la Cuarta Entrevista**



4.3.5. Análisis de datos de la quinta entrevista

Luego del ***análisis de datos realizado en la quinta entrevista***, se han encontrado los siguientes factores que afectan la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la institución.

Respecto de las restricciones en las políticas de gobierno, es necesario dar a conocer técnicamente la norma de seguridad 27001, ya que no es una norma que está únicamente centrada en informática; sin embargo, y dado el desconocimiento existente, se le asocia mucho a lo que es TI. En este sentido, ha sido la ONGEI la entidad que ha tomado la iniciativa con la publicación de la norma. Además, periódicamente se congrega a los oficiales de seguridad para orientarlos. Por otro lado, hay una iniciativa de la ONGEI que se llama PeCERT y que busca dar apoyo a las entidades del Estado en cuanto a incidentes de seguridad. *"Hay que tomar la parte positiva, están convocando, están incentivando a través de legislaciones, a través de información a que se concientice la seguridad"*.

Un factor que se presenta actualmente es que es el oficial de seguridad el que tiene que convencer a la Alta Dirección, cuando debería ser alguien que esté más arriba y explicarle a la Alta Dirección de las instituciones públicas la importancia de este tema. *"La ONGEI llega a los oficiales de seguridad y a los gerentes de TI, pero estos no son decisores, no otorgan recursos"*.

Otro problema que se presenta es que no existe el cargo de Oficial de Seguridad en la estructura orgánica de las entidades públicas, donde generalmente estos son CAS (contratos no permanentes).

Finalmente, respecto del apoyo que brinda el Estado para el SGSI podemos decir que todo parte de la decisión política. *"Estamos avanzando, debemos ver los inicios no como lo mucho que nos falta sino como lo importante de haber empezado"*.

Respecto de las restricciones en la parte operativa:

- En relación a la gestión, se afirma que siendo la información el activo más importante de una entidad pública, este merece ser resguardado, cuidado y protegido. Sin embargo, hay otros impactos más fuertes que como no se ven, no se valorizan y que deberían tomarse más en cuenta. *"Actualmente las instituciones públicas están abordando el tema de la seguridad de la información por el lado de la imagen, 'del no quedar mal', por el lado de que no me hackeen mi página web, y eso es la mínima parte, digamos que el impacto más preocupante se centra en la imagen"*.

  Por otro lado, las estrategias que vienen implementando las entidades públicas siguen siendo diversas. En este caso, la estrategia que se trazó fue implementar el SGSI como piloto en el área de TI, la cual es un área en la que se pueden implementar normas y directivas y realizar ensayo-error. Posteriormente, como parte de la maduración organizacional, ya seguridad de la información pasará a otra área sabiendo cómo es que funciona en TI. *"A nuestro parecer una buena estrategia es que, inicialmente, seguridad de la información esté en el área de TI para que seguridad, estando dentro, pueda arreglar la casa"*.

  Además, se ha creado una página web de seguridad de la información que está dentro de la intranet a través de un icono de seguridad de la información y donde aparece una presentación del oficial de seguridad, con los puntos principales de porqué es importante la seguridad, algunos videos y las normativas que se están aprobando.

  Otro factor que viene afectando enormemente es que las instituciones públicas son organizaciones funcionales y no están organizadas por procesos.

Sin embargo, la NTP 27001 establece, como punto de partida, que la institución funcione por procesos. Es decir que se asume que la organización funciona por procesos. El problema está en que nuestras organizaciones no funcionan por procesos, sino por funciones.

Así que, orientar el SGSI a una estrategia por procesos es complicado; sin dejar de lado que generalmente, sus mapas de procesos (MAPRO) están desactualizados.

- En relación al apoyo institucional, hay que tener en cuenta que el punto de partida primordial para implementar un SGSI es el respaldo de la Alta Dirección. *"Para que la Alta Dirección de una institución pida presupuesto adicional tiene primero que comprarse la idea de que la seguridad de la información es importante"*.

  A pesar de que la Alta Dirección sabe de su importancia todavía no lo asocian a un asunto de presupuesto. Por tanto, la piedra angular es el respaldo de la Alta Dirección.

- En relación a la organización del SGSI, el factor más importante para que no se haya podido implementar hasta ahora en el Estado es la falta de conciencia. Aún estamos tomando conciencia lentamente de la importancia de la seguridad de la información. En general no se capacita, no hay una cultura a nivel de las instituciones públicas de capacitar al personal, porque además tienen el presupuesto limitado y no hay la cultura de invertir en capacitación.

  Respecto del presupuesto, se puede concluir que aún no hay la asociación de importancia vs costo. La Alta Dirección sabe que es importante la implementación del SGSI, pero todavía no lo asocian al desembolso de

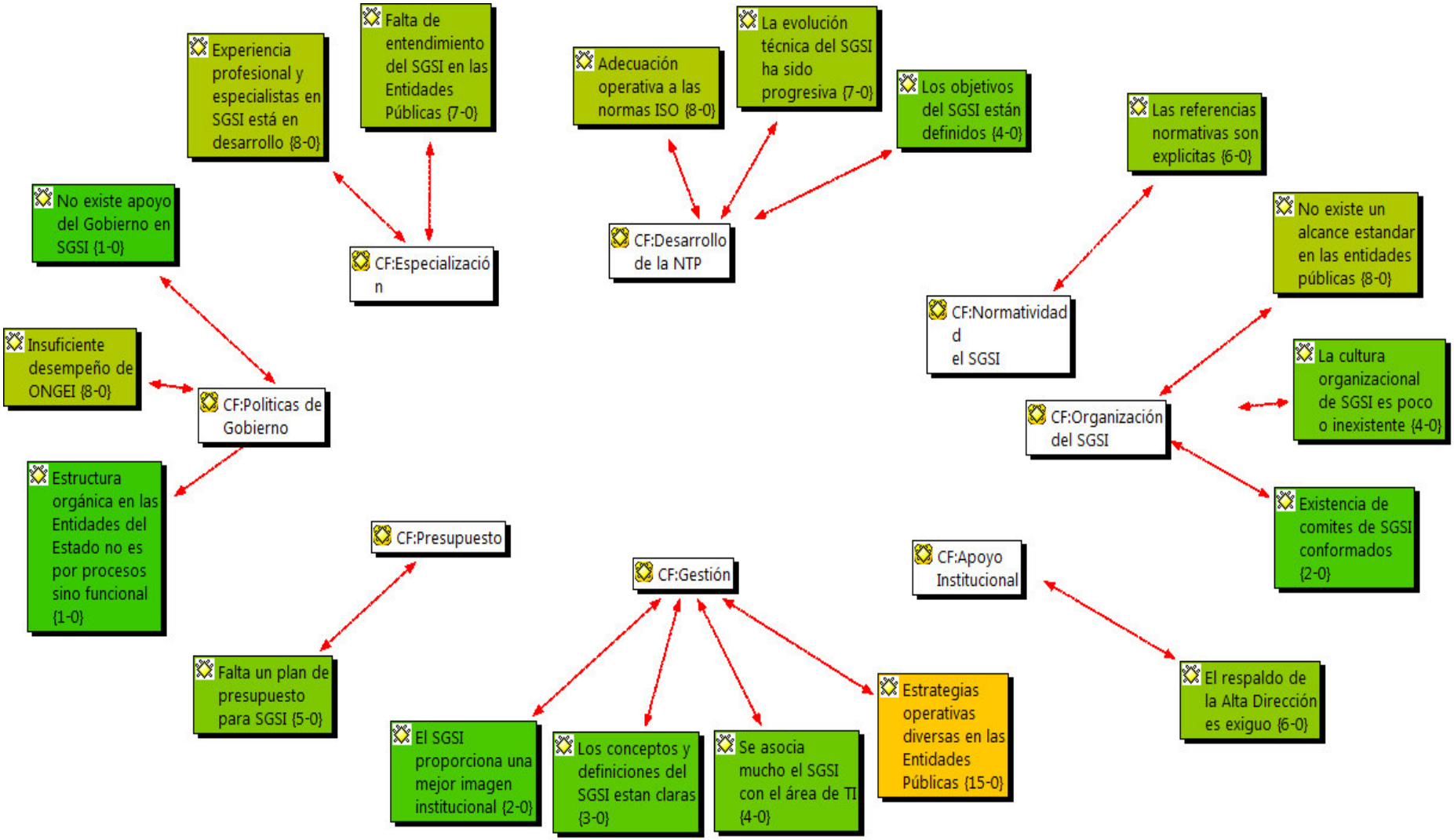
recursos. Esta falta de conciencia hace que las instituciones públicas no dispongan recursos económicos para la implementación de la seguridad de la información en sus instituciones.

En el siguiente cuadro podemos visualizar un resumen de los factores y sus indicadores encontrados en la quinta entrevista:

Factores que afectan la implementación del SGSI en las entidades públicas	Indicadores encontrados en la 5ta. Entrevista	N° incid
1. Políticas de Gobierno	1.1. Insuficiente desempeño de la ONGEI	4
	1.4. Estructura orgánica y funcional del Oficial de Seguridad en las Entidades del Estado	2
	1.5. Existe apoyo del Gobierno para SGSI	2
2. Desarrollo de la NTP	2.1. Los objetivos están definidos	1
	2.3. Falta de adecuación operativa a las normas standard ISO	1
3. Presupuesto	3.1. Falta un plan de presupuesto para SGSI.	6
5. Gestión del SGSI	5.3. Los conceptos y definiciones del SGSI están claros	2
	5.4. Estrategias Operativas diversas en las instituciones	7
	5.7. La estructura orgánica en las entidades del Estado no es por procesos sino funcional	4
	5.8. Se asocia mucho SGSI con el área de TI (creencia que TI debe implementar)	2
6. Apoyo Institucional	6.1. El respaldo de la Alta Dirección es exiguo (x desconocer importancia)	10
8. Organización del SGSI	8.1. No se define un alcance estandarizado en las instituciones (generalmente es el DC)	1
	8.2. Ya existen comités de SGSI conformados	2
	8.4. La cultura organizacional del SGSI es poca o inexistente	4

Tabla N° 9: **Identificación de los indicadores encontrados en la Quinta Entrevista en cada uno de los factores formulados**

Gráfico N° 17: **Diagrama de Análisis de Datos de la Quinta Entrevista**



4.3.6. Análisis de datos de la sexta entrevista

Luego del ***análisis de datos realizado en la sexta entrevista***, se han encontrado los siguientes factores que afectan la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la institución.

Respecto de las restricciones en las políticas de gobierno, se concluye que la ONGEI no es una oficina con representatividad política propia, no tiene la fuerza suficiente para la ejecución de las normas que dicta. Sin embargo, se tiene en cuenta también que esta entidad ha hecho un buen trabajo con la NTP ya que las entidades por sí mismas nunca iban a aplicarlo. *"El problema es que ONGEI es una entidad pequeña, le falta la fuerza como para que dirija y oriente con mayor fuerza a las entidades del Estado"*.

Finalmente, se agrega que otro de los factores que afectan a la NTP, es el tiempo que toman los procesos de adquisición de los elementos que se requieren para el plan de seguridad de información, sobre todo cuando son complejos o de montos altos. Se recomienda que dichas adquisiciones, por temas de seguridad de información, deberían tener un marco legal diferente, ser exonerados tal vez de algunos procesos o de menor tiempo en sus plazos, pero siendo totalmente transparente con las convocatorias.

Respecto de las restricciones de desarrollo de la NTP, se destaca la facilidad que otorga la norma ya que trata de que todas las entidades realicen actividades de seguridad de una manera estándar, siguiendo los lineamientos que les permita proteger su información en diferentes aspectos en los 11 dominios de dicha norma.

Otro de los problemas que se enfrentó esta entidad es que todo lo desarrollado hasta el momento es bastante nuevo en la implementación de la NTP, y esto le pasa también a otras entidades públicas; teniendo en cuenta que ya en un segundo ciclo de

la norma, ésta se hará con mayor conocimiento y hasta con mejoras, haciendo más sólidas las cosas.

Un problema que también se ha presentado es que, para cumplir las actividades del plan de seguridad de información y que involucra a otras áreas, a veces hay que lidiar con el plan de trabajo de estas áreas que ya lo tienen definido.

Respecto de las restricciones en la parte operativa:

- En relación a la gestión, si bien inicialmente existía un desconocimiento respecto de la operatividad de la NTP, cuando se fue entendiendo la magnitud y la implicancia, los miembros del comité de seguridad tomaron conciencia de que es un tema institucional no solamente tecnológico y se aperturaron las facilidades para conseguir un mayor presupuesto.

  Además, la norma permite, como es un ciclo de mejora continua, empezar por partes e ir creciendo. En un principio, por las mismas etapas que tiene el ciclo de vida de la norma, una de las primeras fases era hacer un análisis de riesgo, definición del alcance, identificación de los controles, actividades que mitiguen los riesgos. *"Toda esa parte era cómo de análisis. Ya cuando producto de ello, se determina el plan de acción es que ya comienzan a salir actividades concretas que son visualizadas por el comité de seguridad de la información".*

  Actualmente hay muchas entidades que por desconocimiento de los procesos que tienen no resguardan bien su información, no la protegen. Hay muchos procesos, que también escapan de lo tecnológico, y se requieren coordinaciones con otras áreas. Debido a ello, en la OGTI de esta entidad se identificaron qué procesos estaban débiles y qué procesos faltaban documentar.

Por tanto, una recomendación es que se debería aplicar en las organizaciones una implementación de la ISO 9001, ya que esto asegura la calidad de los procesos durante todo el ciclo del mismo.

Sin embargo, en nuestro caso, cuando apareció la norma, se tuvo que aplicarla con los procesos que se tenían, ya que certificar primero un proceso y madurarlo como lo pide un ISO 9001, requería de mucho tiempo y los riesgos que podían presentarse eran muy peligrosos.

- En relación al apoyo institucional, uno de los factores que viene influyendo es el entendimiento que puedan tener las áreas no informáticas de la entidad y la Alta Dirección de la misma para apoyar a la Oficina de Informática que permita desarrollar esta norma. Este apoyo por parte de la Alta Dirección se viene dando debido a que han entendido la importancia que tiene esta norma.

- En relación a la normatividad, el principal factor es que los miembros del comité de seguridad de información entiendan primero lo que significaba la norma, y para son necesarias muchas reuniones de coordinación y de explicación.

  Sin embargo, con la NTP las instituciones tienen una guía para que -en base a los controles que hay que cumplir- puedan planificar todas las acciones que hay en el corto, mediano o largo plazo y asegurar de esa manera que los procesos sean correctos y con calidad.

- En relación a la organización del SGSI, un factor restrictivo para la implementación de la NTP es principalmente la cultura organizacional respecto de la implementación del SGSI, lo cual es parte de un proceso de concientización de las personas que no están relacionadas con la norma.

> Los talleres de sensibilización que se desarrollen deben ser bastante didácticos, explicando principalmente los diferentes riesgos existentes de no cuidar la información que manejan. Es necesario para ello mantener una coordinación muy extensa para las diferentes áreas de la organización entiendan que la aplicación de la norma va más allá de lo tecnológico.

Respecto del presupuesto, no ha sido fácil lograr un presupuesto propio para el SGSI como es actualmente. *"En un principio no se tuvo presupuesto, pero luego cuando ya se aprobó el plan de seguridad de la información del presente año (2015) y, al haber sido aprobado por todos los miembros del comité de seguridad, se le buscó un presupuesto"*.

Antes de ello fue necesario utilizar el presupuesto de la OGTI, cubriéndose actividades del SGSI con presupuesto de la oficina de TI, lo cual restaba recursos al área y no se podían desarrollar las actividades del SGSI en el tiempo previsto ya que era un presupuesto inseguro.

Respecto de la especialización, es necesario hacer hincapié en la importancia de entender el concepto de la implementación de la NTP en la organización para que, a partir de allí, exista el apoyo necesario de todos los trabajadores de la institución en seguir los lineamientos que dice la norma.

Una estrategia utilizada por esta entidad para realizar talleres de sensibilización de seguridad de la información a todo el personal, es contratar a una empresa especializada que venga con un temario bien definido incluyendo afiches para su difusión referidos a la seguridad de información con diferentes recomendaciones y que lo repliquen en sus oficinas *"y hasta en sus hogares"*.

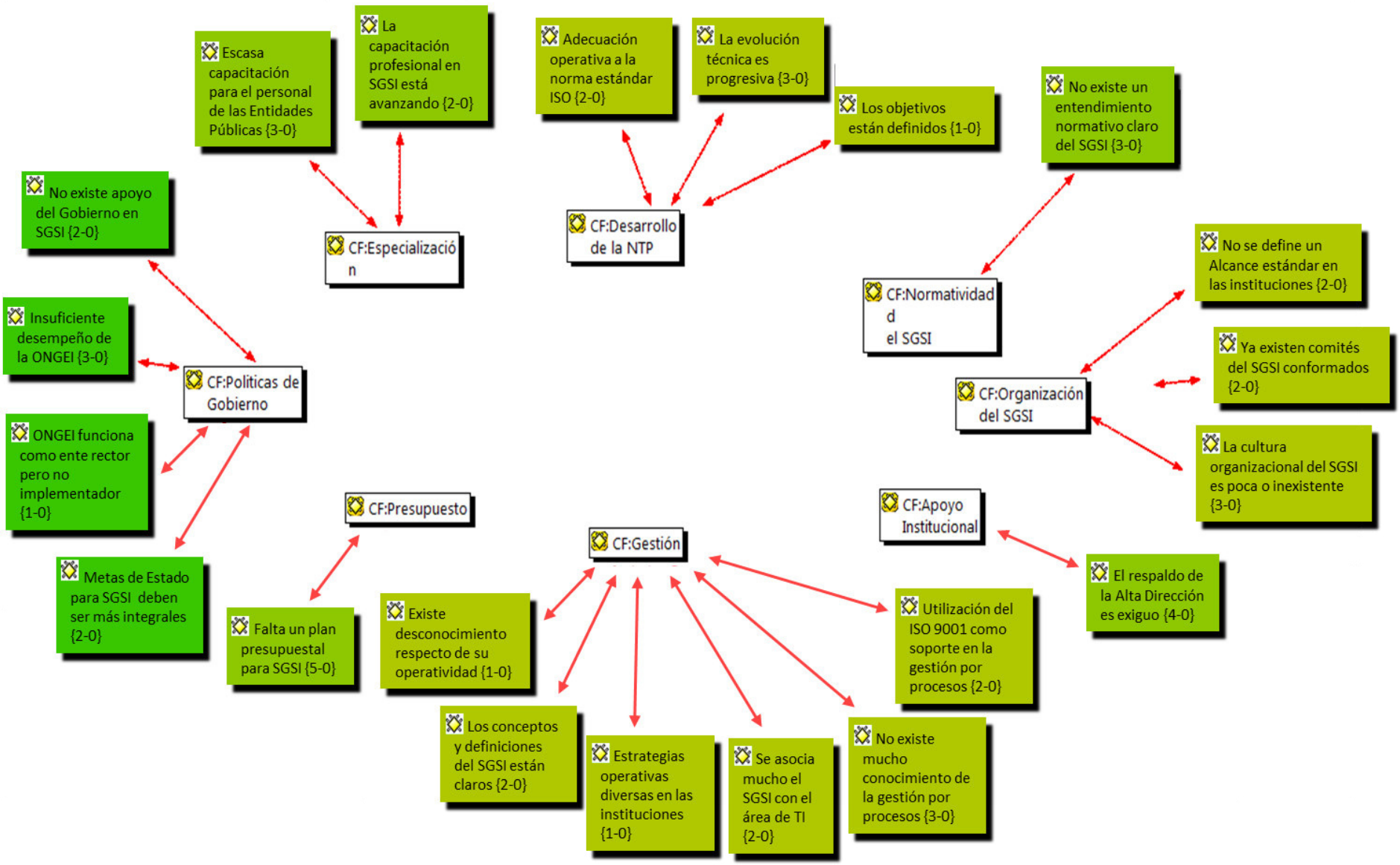
Respecto de la capacitación profesional de especialistas en SGSI se han realizado talleres de capacitación para el personal de la oficina de TI, tanto para los desarrolladores, operadores y directivos.

En el siguiente cuadro podemos visualizar un resumen de los factores y sus indicadores encontrados en la sexta entrevista:

Factores que afectan la implementación del SGSI en las entidades públicas	Indicadores encontrados en la 6ta. Entrevista	N° incid.
1. Políticas de Gobierno	1.1. Insuficiente desempeño de la ONGEI	3
	1.3. Metas de Estado para el SGSI deben ser más integrales	2
	1.5. Existe apoyo del Gobierno para SGSI	2
	1.6. ONGEI funciona como ente rector pero no implementador	1
2. Desarrollo de la NTP	2.1. Los objetivos están definidos	1
	2.2. La evolución técnica es progresiva	3
	2.3. Adecuación operativa a la norma standard ISO	2
3. Presupuesto	3.1. Falta un plan presupuestal para SGSI	5
4. Especialización	4.1. Escasa capacitación para el personal de las Entidades Públicas	3
	4.4. La capacitación profesional de especialistas en SGSI está avanzando	2
5. Gestión del SGSI	5.2. Existe desconocimiento respecto de su operatividad	1
	5.3. Los conceptos y definiciones del SGSI están claros	2
	5.4. Estrategias Operativas diversas en las instituciones	1
	5.8. Se asocia mucho SGSI con el área de TI (creencia que TI debe implementar)	2
	5.9. No existe mucho conocimiento de la gestión por procesos	3
	5.11. Utilización del ISO 9001 como soporte en la gestión por procesos	2
6. Apoyo Institucional	6.1. El respaldo de la Alta Dirección es exiguo (x desconocer importancia)	4
7. Normatividad del SGSI	7.1. No existe un entendimiento normativo claro del SGSI	3
8. Organización del SGSI	8.1. No se define un alcance estandarizado en las instituciones (generalmente es el DC)	2
	8.2. Ya existen comités de SGSI conformados	2
	8.4. La cultura organizacional del SGSI es poca o inexistente	3

Tabla N° 10: **Identificación de los indicadores encontrados en la Sexta Entrevista en cada uno de los factores formulados**

Gráfico N° 18: **Diagrama de Análisis de Datos de la Sexta Entrevista**



4.3.7. Análisis de datos de la séptima entrevista

Luego del ***análisis de datos realizado en la séptima entrevista***, se han encontrado los siguientes factores que afectan la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la institución.

Respecto de las restricciones en las políticas de gobierno, se concluye que la ONGEI es una entidad que viene cumpliendo el rol de incentivar o fomentar la implementación de la norma –a través del apoyo técnico en la solicitud y revisión de los planes de trabajo para la ejecución del SGSI en las entidades públicas- se aprecian limitaciones operativas principalmente de personal y funcional.

Además se hace una mención a que con la norma anterior no había tanto apoyo técnico y se espera que con esta nueva norma la ONGEI tenga una mayor representatividad en forma integral con las entidades públicas.

Finalmente se agrega que, otro de los factores que podrían afectar a la implementación de la norma es la actual coyuntura política, ad-portas de un cambio de gobierno, lo que podría traer cambios en esta entidad y de objetivos estratégicos para la implementación del SGSI.

Respecto de las restricciones de desarrollo de la NTP, se puede apreciar que los objetivos que busca la NTP de seguridad de la información están claramente definidos y así lo han percibido los oficiales de seguridad entrevistados. Se tiene también una visión clara respecto de las funciones asignadas y el papel que cumple la norma en apoyo de la organización y sobretodo de cómo podría ayudar a mitigar los riesgos informáticos y de continuidad de negocios. *"Ahora estamos previendo los ataques informáticos, cómo tenemos que estar preparados, qué procedimientos se deben hacer, cómo debemos actuar ante esto, cómo hacer que los servicios tecnológicos dentro de la instituciones no paren"*.

Por tanto esta norma va a ser beneficiosa para todas las entidades del Estado que lo apliquen y que tengamos conocimiento de cómo actuar.

Un factor que también podría afectar es que no hay una comprensión cabal de que esta nueva norma se adecúa operativamente con otras normas ISO. "Estoy revisando la NTP 27001 y estoy viendo que se relaciona con otras normas ISO como son la de riesgos, la ISO 31000 y también con COBIT".

Respecto de las restricciones en la parte operativa:

- En relación a la gestión, se mantiene aún un desconocimiento respecto de la operatividad de la NTP, pero con esta nueva norma se va optimizando la ejecución de la misma. Sin embargo, se hace referencia a que existen estrategias operativas diversas en las instituciones del Estado. Las metodologías de gestión de riesgos, por ejemplo, son diversas, y generalmente son de elaboración propia. *"Para la identificación de riesgos estamos utilizado una metodología propia, la cual tiene que ver con ponderaciones que nos permitan identificar los activos con los riesgos más críticos"*. Esta incidencia que se presenta acá es un factor que se repite en todas las entrevistas realizadas, lo cual denota la falta de integración en el SGSI de las entidades públicas.
- En relación al apoyo institucional, se hizo mención de que si bien hay un respaldo de la Alta Dirección, aún hay mucho desconocimiento de los beneficios o problemas que podría causar una incorrecta o nula implementación de la seguridad de la información en la institución.

  Hace falta más concientización en la Alta Dirección al respecto. *"Ellos tienen una idea básica de qué cosa es seguridad de la información pero muy clara todavía"*.

- En relación a la normatividad, el principal factor que afecta la implementación del SGSI es que los miembros del comité de seguridad de información entiendan claramente que significa la norma cómo beneficia a la institución, y para son necesarias muchas reuniones de coordinación y presentaciones puntualizando estos aspectos.
- En relación a la organización del SGSI, un factor limitante para la implementación de la NTP es principalmente la cultura organizacional por parte del personal de la institución, el cual –como en todas las demás instituciones del Estado- es muy incipiente. La cultura organizacional en seguridad de la información en el personal no es un tema prioritario para as personas. No existe directamente concienciación en este tema para el personal, hay que empezar desde cero. "*El personal de esta institución actualmente no tiene una cultura organizacional en seguridad de la información. Tienen una idea muy básica.*". Igualmente, las estrategias a utilizar son propias, no hay una estrategia integral en este campo.

  Respecto del alcance, se hizo referencia a que no existe un alcance estandarizado al respecto, más aún que la NTP vigente deja a criterio de la organización esta posibilidad. Es decir, se podría tomar como alcance un área, proceso, macro-proceso, una dirección general; ahí es que con más énfasis debería haber unos lineamientos por parte del ente rector.

Respecto del presupuesto, como muchas de las entidades entrevistadas éste es un punto crítico. No se cuenta con presupuesto adicional para el SGSI salvo el remunerativo del personal encargado de la implementación. *"Básicamente nosotros no contamos con presupuesto, por eso es que toda implementación que hemos*

realizado durante esta última gestión ha sido en base a las remuneraciones del personal encargado para este proyecto".

Respecto de la especialización, se ha hecho referencia a que un factor importante es la poca capacitación que brinda la ONGEI a las entidades públicas, la cual habría que incrementarla a través de programas anuales de formación de especialistas en SGSI para el Estado.

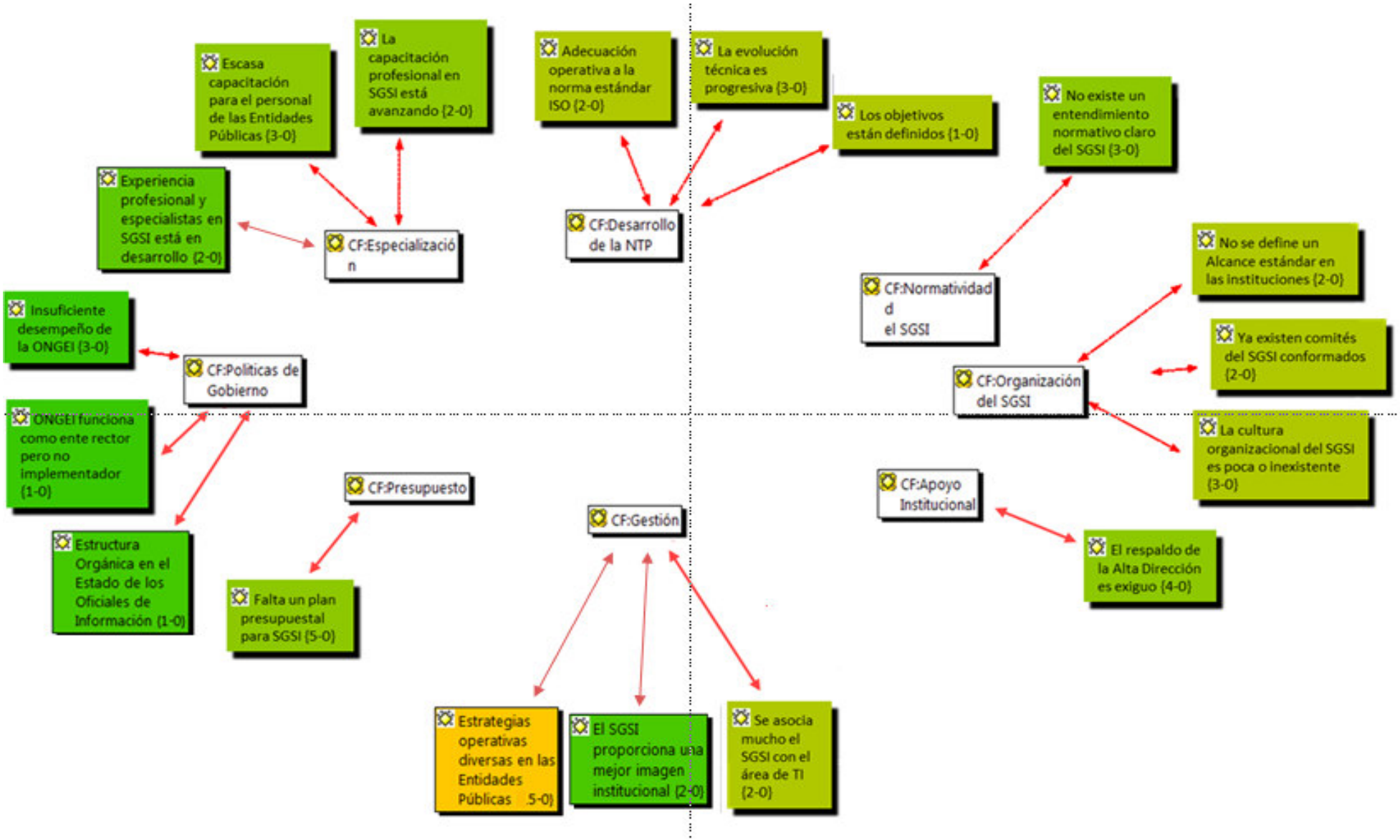
> Otro de los factores es el de personal con especialización en SGSI, el cual su asignación muchas veces no es técnica. *"Un factor podría ser elegir un personal especializado en seguridad de información y no a cualquier personal que no tenga conocimientos en SGSI"*.
>
> Otro problema que está relacionado al presupuestal es la poca capacitación que tiene el personal de la institución en seguridad de la información.

En el siguiente cuadro podemos visualizar un resumen de los factores y sus indicadores encontrados en la séptima entrevista:

Factores que afectan la implementación del SGSI en las entidades públicas	Indicadores encontrados en la 7a. Entrevista	N° incid
1. Políticas de Gobierno	1.1. Insuficiente desempeño de la ONGEI	2
	1.4. Estructura orgánica y funcional del Oficial de Seguridad de la información en las Entidades del Estado	2
	1.6. ONGEI funciona como ente rector pero no implementador	1
2. Desarrollo de la NTP	2.1. Los objetivos están definidos	2
	2.2. La evolución técnica es progresiva	5
	2.3. Adecuación operativa a la norma standard ISO	1
3. Presupuesto	3.1. Falta un plan presupuestal para SGSI	2
4. Especialización	4.1. Escasa capacitación para el personal de las Entidades Públicas	2
	4.2. La experiencia profesional del SGSI aún está en desarrollo	3
	4.4. La capacitación profesional de especialistas en SGSI está avanzando	2
5. Gestión del SGSI	5.4. Estrategias Operativas diversas en las instituciones	2
	5.5. El SGSI proporciona una mayor imagen institucional	2
	5.8. Se asocia mucho SGSI con el área de TI (creencia que TI debe implementar)	2
6. Apoyo Institucional	6.1. El respaldo de la Alta Dirección es exiguo (x desconocer importancia)	2
7. Normatividad del SGSI	7.1. No existe un entendimiento normativo claro del SGSI	1
8. Organización del SGSI	8.1. No se define un alcance estandarizado en las instituciones (generalmente es el DC)	2
	8.2. Ya existen comités de SGSI conformados	2
	8.3. No existe un nivel de avance del SGSI muy desarrollado en las entidades públicas	2
	8.4. La cultura organizacional del SGSI es poca o inexistente	5

Tabla N° 11: ***Identificación de los indicadores encontrados en la Séptima Entrevista en cada uno de los factores formulados***

Gráfico N° 19: **Diagrama de Análisis de Datos de la Séptima Entrevista**



4.4. Conclusiones y discusión del análisis de datos

Luego de la recolección de datos a través de la realización de entrevistas a profundidad, su transcripción y el análisis de los mismos, se han obtenido un conjunto de variables por cada factor establecido, que nos representan los principales indicadores que el investigador ha ido encontrando luego de una revisión exhaustiva de dichas entrevistas.

Además, y a efectos de consolidar la información procesada, se está agregando un cuadro consolidado respecto de los indicadores que han afectado en forma positiva y negativa, para cada uno de los factores encontrados en la investigación.

Así también, teniendo en cuenta las investigaciones encontradas en el Capítulo II respecto de los factores que afectan la seguridad de la información a nivel mundial (2.4.5), y en base a las conclusiones obtenidas del análisis de datos de las entrevistas del presente trabajo de investigación, se ha realizado un análisis comparativo y discusión respecto de los factores encontrados.

4.4.1. Procedimiento

Con la finalidad de establecer un parámetro de valoración a los indicadores encontrados, se ha identificado -en cada una de las entrevistas realizadas- el número de incidencias que se han presentado en estos indicadores, y que nos permita asignar el grado de importancia de cada una de estas, que tomará trascendencia en la determinación de las conclusiones finales.

Por ello, se ha elaborado una matriz de evaluación por cada factor propuesto, a través de la identificación de métricas y ponderación de los incidencias presentadas

tomando como base los "indicadores encontrados en las entrevistas realizadas" para el presente trabajo de investigación.

4.4.2. Matriz de evaluación de incidencias de los factores encontrados

A) Evaluación del factor: Políticas de Gobierno

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
1. Políticas de Gobierno	**1.1. Insuficiente desempeño de la ONGEI**	1	1	2	1	4	3	2	**14**
	1.2. Constantes cambios en las Políticas de Estado	1	1	2	-	-	-	-	4
	1.3. Metas de Estado para el SGSI más integrales	-	3	4	-	-	2	-	**9**
	1.4. Estructura organizacional y funcional del Oficial de Seguridad en las Entidades Públicas	1	1	2	1	2	-	2	**9**
	1.5. No existe suficiente apoyo del Gobierno en implementar el SGSI	-	-	-	1	2	2	-	5
	1.6. ONGEI funciona como ente normativo pero no implementador	-	-	-	3	-	1	1	4

Tabla N° 12 - **Relación entre los indicadores de las Políticas de Gobierno (Factor 1) y el número de incidencias presentadas en las entrevistas**

Factor Políticas de Gobierno	
Indicadores negativos - Insuficiente desempeño de la ONGEI - Constantes cambios en las Políticas de Estado - Metas de Estado para el SGSI más integrales - Estructura organizacional y funcional del Oficial de Seguridad en las Entidades - No existe suficiente apoyo del Gobierno en la implementación del SGSI - ONGEI funciona como ente normativo pero no implementador.	**Indicadores positivos** - No se encontraron

Del análisis realizado en las entrevistas, se puede inferir que el principal problema que se presenta en las Políticas de Estado es que el desempeño de la ONGEI es insuficiente respecto de la implementación del sistema de gestión de seguridad de la información en las entidades públicas, ya que si bien viene cumpliendo un papel normativo, no está haciendo un papel como ente implementador.

Esta entidad debería tomar acciones que permitan la articulación entre las entidades, sobre todo en aquellas ya certificadas las cuales pudieran enseñar a otras entidades que aún están en la etapa de implementación. Además, sería de mucha importancia que también pudiera reunir a todas las altas autoridades del Estado y brindarles una capacitación en SGSI, teniendo en cuenta que la seguridad de la información es un objetivo estratégico de una Política de Estado.

De las entrevistas realizadas, se hace mención respecto de la creación de un set de profesionales especialistas en SGSI que puedan dar el soporte necesario y monitoreen el avance de la NTP en las entidades públicas. Para ello, es necesario que esta NTP esté contemplada como una Política Nacional de Seguridad de la Información que cuente con representatividad y presupuesto propio.

Asimismo, las metas de estado respecto del SGSI deben ser más integrales y estar orientadas a la necesidad de interactuar entre las entidades enmarcadas en la NTP. Es necesario desarrollar un plan de seguridad nacional que permita optimizar el uso de recursos y unificación de esfuerzos interinstitucionales.

Así también deberían aplicarse medidas especiales, como un marco legal específico para los procesos de adquisición de los elementos que se requieren para la

ejecución del plan de seguridad de información, sin perder la transparencia en dichas convocatorias.

Finalmente, los entrevistados coinciden en la formalización del cargo del Oficial de Seguridad de la Información en la estructura funcional de la organización en los documentos de gestión institucional como son el ROF y MOF, lo que permitirá contar con un cargo designado en la entidad y un presupuesto. Este cargo además no debería depender del área de informática u otra área funcional sino de la Alta Dirección directamente.

Estas conclusiones descritas pueden confirmarse con las investigaciones encontradas respecto del análisis de los factores de seguridad de la información a nivel mundial en el Capítulo II (2.4.5), en el *caso de estudio de los factores que influyen en la gestión de la seguridad de la información en empresas pequeñas y medianas en Turquí*a (Yeniman, 2011) donde una de las conclusiones a las que llega este estudio afirma que uno de los factores importantes es el apoyo que brinda la Alta Dirección a las políticas de seguridad de información institucional.

En otro estudio denominado *"los 10 pecados capitales de la gestión de la seguridad de la información"* (Solms, 2004), se afirma que es esencial una estructura organizativa adecuada de gobierno de seguridad de la información.

Finamente en el estudio denominado: *"Roles ejecutivos del comité de seguridad de la información"* (Williams, 2007), se exploran los diferentes roles y responsabilidades que debe afrontar el oficial de seguridad de la información para contribuir a una implementación exitosa, y donde se reconoce el hecho de integrar funciones del oficial dentro de una entidad holística capaz de reaccionar ante cualquier amenaza a la información.

B) Evaluación del factor: Desarrollo de la NTP

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
2. Desarrollo de la NTP	2.1. Los objetivos del SGSI están claramente definidos	1	-	2	1	1	1	2	8
	2.2. La evolución técnica es progresiva	1	-	-	-	-	3	4	8
	2.3. Falta de adecuación operativa a la norma estándar ISO	1	2	1	1	1	2	1	**9**

Tabla N° 13 – **Relación entre los indicadores del Desarrollo de la NTP (Factor 2) y el número de incidencias presentadas en las entrevistas**

Factor Desarrollo de la NTP	
Indicadores negativos	**Indicadores positivos**
- Falta de adecuación normativa a la norma estándar ISO	- Los objetivos del SGSI están claramente definidos - La evolución técnica es progresiva

El principal problema que se ha presentado en las entrevistas respecto del Desarrollo de la NTP, es la falta de adecuación operativa de las normas internacionales ISO por parte de las entidades públicas, lo que involucra también a la NTP-ISO/IEC 27001. La implementación del SGSI está más enfocada a temas de seguridad en los sistemas informáticos o en los sistemas de comunicación de datos.

Por otro lado, las entidades públicas no tienen mayor experiencia en el desarrollo de las fases de la NTP y esto trae complicaciones en la ejecución operativa del SGSI. Así también, cuando se involucra a otras áreas de la entidad hay que lidiar con su plan de trabajo, el cual no contempla generalmente actividades de ejecución del SGSI generándose problemas de coordinación. Una de las buenas prácticas que se pudo rescatar de las entrevistas a las entidades que ya certificaron en SGSI, es la experiencia obtenida en el desarrollo de procesos basados en la ISO 9000. Esto ha permitido cultivar una cultura sobre los sistemas de gestión.

C) Evaluación del factor: Presupuesto del SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
3. Presupuesto	3.1. Falta de un plan presupuestal para el SGSI	1	3	2	1	6	5	2	20

Tabla N° 14 – **Relación entre los indicadores de Presupuesto (Factor 3) y el número de incidencias presentadas en las entrevistas**

Factor Presupuesto	
Indicadores negativos	**Indicadores positivos**
- Falta de un plan presupuestal para el SGSI	- No se encontraron

Un factor muy importante, que se ha presentado en las entrevistas realizadas, es la falta de un plan presupuestal para el SGSI. Esto se debe principalmente a que las entidades públicas no han tenido un conocimiento exacto de cómo implementar presupuestalmente la NTP relativa a la seguridad de la información. Incluso, muchas de ellas actualmente cubren las actividades del SGSI generalmente con presupuesto de las áreas de TI. Otro aspecto a considerar es que si bien la Alta Dirección de las entidades públicas ya está tomando conciencia de la importancia respecto de la implementación del SGSI, aún no logran relacionarlo con el desembolso de recursos. Es decir, aún no hay la asociación importancia vs costo.

Finalmente, hay que tener en cuenta que la implementación del SGSI en una organización no es solamente la inversión en el costo de implementación del proyecto, sino que también tiene un costo de mantenimiento y esto incluye tener a un equipo de personas destinadas a tiempo completo a cumplir con actividades de gestión propias del SGSI empezando por formalizar al oficial de seguridad de la información en las instituciones públicas.

D) Evaluación del factor: Especialización en SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
4. Especiali-zación	4.1. Escasa capacitación del SGSI para el personal de las entidades públicas	1	-	-	1	-	3	2	7
	4.2. La experiencia profesional del SGSI aún está en desarrollo	1	3	1	1	-	-	2	**8**
	4.3. La capacitación profesional de especialistas en SGSI está avanzando	-	-	1	-	-	2	2	5
	4.4. Formación de equipos profesionales interinstitucionales en seguridad de información	-	-	-	1	-	-	-	1

Tabla N° 15 – **Relación entre los indicadores de la Especialización (Factor 4) y el número de incidencias presentadas en las entrevistas**

Factor Especialización	
Indicadores negativos	**Indicadores positivos**
- Escasa capacitación del SGSI para el personal de las entidades públicas - La experiencia profesional del SGSI aún está en desarrollo - (falta de) Formación de equipos profesionales interinstucionales en seguridad de información	- La capacitación profesional de especialistas en SGSI está avanzando

Otro de los factores que se presenta es la falta de profesionales especializados en la implementación del SGSI, lo cual es muy escaso en nuestro país. Normalmente el cargo de Oficial de Seguridad de la información (OSI) recae en un profesional sin la experiencia ni la capacitación necesaria en este tipo de tareas, afín de que sea un interlocutor entre la Alta Dirección y las dependencias de la institución.

Es necesario, por tanto, contar con un staff de especialistas peruanos y extranjeros con conocimientos avanzados en este tema, los cuales no sólo tendrían como objetivo el monitoreo y avance de las entidades públicas, sino también la labor de formar especialistas certificados internacionalmente en seguridad de la información.

D) Evaluación del factor: Gestión del SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
5. Gestión del SGSI	5.1. Existe desconocimiento respecto de su operatividad	2	-	2	-	-	1	-	5
	5.2. Los conceptos y definiciones del SGSI están claros	-	2	-	-	2	2	-	6
	5.3. Estrategias operativas diversas en las entidades públicas	2	3	2	3	7	1	2	**20**
	5.4. El SGSI proporciona una mejor imagen institucional	1	-	-	-	-	-	1	1
	5.5. El mapa de procesos en las instituciones públicas está desactualizado	-	4	2	-	-	-	-	6
	5.6. La estructura orgánica en las entidades públicas es funcional y no por procesos	-	-	-	-	4	-	-	4
	5.7. Se asocia mucho la implementación del SGSI con el área de Tecnologías de Información (TI)	1	2	1	3	2	2	2	**13**
	5.8. No existe mucho conocimientos de la gestión por procesos	1	-	-	2	-	3	3	6
	5.9. Existen mayores riesgos en las entidades públicas debido al incremento del uso de las TIC	1	-	-	1	-	-	-	2
	5.10. Utilización del ISO 9001 como soporte de la gestión por procesos	3	-	-	3	-	2	-	**8**

Tabla N° 16 – **Relación entre los indicadores de la Gestión del SGSI (Factor 5) y el número de incidencias presentadas en las entrevistas**

Factor Gestión del SGSI	
Indicadores negativos	**Indicadores positivos**
- Existe desconocimiento respecto de su operatividad - Estrategias operativas diversas en las entidades públicas - El mapa de procesos en las instituciones públicas está desactualizado - La estructura orgánica en las entidades públicas es funcional y no por procesos - Se asocia mucho la implementación del SGSI con el área de TI - No existe mucho conocimiento de la gestión por procesos - Existen mayores riesgos en las entidades públicas debido al incremento de las TIC	- Los conceptos y definiciones del SGSI están claros - El SGSI proporciona una mejor imagen institucional - Utilización del ISO 9001 como soporte de la gestión por procesos

Respecto del factor de Gestión del SGSI, se puede concluir que las estrategias operativas de implementación de la NTP en las instituciones públicas son diversas, donde algunas están más desarrolladas que otras, no existiendo una estrategia de gestión de conocimientos de aquellas entidades públicas que están más avanzadas. Actualmente las instituciones del Estado están trabajando cada una por su lado, buscando sus propios consultores y proveedores de servicios que los ayuden en la implementación del SGSI. Una recomendación que se deriva de este problema es que estas entidades deberían trabajar como Gobierno, todas juntas como un equipo con un ente fortalecido que las lidere, monitoree y capacite permanentemente.

Otro problema que se presenta en las instituciones es que normalmente le encargan la implementación del SGSI al área de informática, y donde esta función tendría depender directamente de la Alta Dirección debido a que el primero es más operativo mientras que el segundo es de supervisión. Normalmente se está tomando como un estándar del SGSI en una organización al centro de datos (Data Center) o los sistemas de información, cuando lo óptimo es que éste deba reposar en un proceso core del negocio el cual se encuentra generalmente en las áreas estratégicas y funcionales de la organización.

Otro factor que influye en la implementación de la norma es que generalmente se piensa que la seguridad de la información está asociada netamente a la informática o que es una función de tecnologías de la información. Por ello, muchas entidades públicas limitan la seguridad de la información únicamente al área de informática y eso es erróneo. Esto trae aparejado incluso que el personal de las demás áreas de la organización no se sienta involucrado en el proyecto del SGSI, ya que piensan con toda lógica que es una tarea que comprende a TI.

Finalmente, es muy importante tener los procesos claros al implementar la seguridad de la información, ya que al tener los procesos claros se tiene una visión de negocio y con ello se puede identificar mejor lo que se quiere implementar. Actualmente, hay muchas entidades que por desconocimiento de los procesos que tienen no resguardan bien su información, no la protegen.

Un factor principal es que las instituciones públicas son organizaciones funcionales y no están organizadas por procesos; Sin embargo, la NTP 27001 establece, como punto de partida, que la entidad organice sus actividades por procesos. Por tanto, una recomendación que se obtiene de las entrevistas es que se debería aplicar el ISO 9001 para asegurar la calidad de los procesos durante todo el ciclo de la norma.

Se puede observar que en las entidades que ya certificaron en el SGSI, se ha aplicado la ISO 9001 como base para la implementación de la ISO 27001.

E) Evaluación del factor: Apoyo Institucional del SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
6. Apoyo Institucional	**6.1. El respaldo de la Alta Dirección es exiguo**	4	5	2	2	10	4	2	**29**

Tabla N° 17 – **Relación entre los indicadores de Apoyo Institucional (Factor 6) y el número de incidencias presentadas en las entrevistas**

Factor Apoyo Institucional	
Indicadores negativos	**Indicadores positivos**
- El respaldo de la Alta Dirección es exiguo	- No se encontraron

La conclusión que se puede inferir en este punto es que en la mayoría de las entidades públicas se desconoce la importancia de efectuar la implementación del Sistema de Gestión de Seguridad de Información (SGSI), así como las consecuencias que acarrearía que no se realice la misma. Hay que tener en cuenta que el punto de partida primordial para implementar un SGSI es el respaldo de la Alta Dirección; a pesar de que la ésta sabe de su importancia, todavía no lo asocian a un asunto de presupuesto.

Una de las aportaciones de los entrevistados es que para que la Alta Dirección de una institución otorgue el respaldo necesario para el SGSI tiene que comprarse la idea de que la seguridad de la información es importante. Para ello, un punto primordial a resolver por el Estado es el de "vender" la seguridad de la información en las entidades públicas.

Se recomienda, por tanto, establecer una estrategia de concienciación a todos los directivos de la Alta Dirección de las instituciones públicas explicándoles a detalle la importancia de la implementación del SGSI.

F) Evaluación del factor: Normatividad del SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
7. Normati-vidad del SGSI	**7.1. No existe un entendimiento normativo claro del SGSI**	**-**	**1**	**1**	**-**	**-**	**3**	**2**	**7**

Tabla N° 18 – **Relación entre los indicadores de Normatividad del SGSI (Factor 7) y el número de incidencias presentadas en las entrevistas**

Factor Normatividad del SGSI	
Indicadores negativos **-** No existe un entendimiento normativo claro del SGSI	**Indicadores positivos** - No se encontraron

La conclusión que se puede apreciar en la Normatividad del SGSI es que si bien se tiene claro que el objetivo principal de la norma es proteger la información del Estado, la misma debe ser adecuada a las necesidades de cada institución para que se tome explícitamente lo que se necesita en la entidad, las cuales podrían también organizarse por tamaño o complejidad de las mismas.

G) Evaluación del factor: Organización del SGSI

Factor	Indicadores encontrados en las entrevistas	Nro. incidencias presentadas							Total
		E1	E2	E3	E4	E5	E6	E7	
8. Organización del SGSI	**8.1. No se define un alcance estándar en las entidades públicas**	**3**	**3**	**2**	**1**	**1**	**2**	**2**	**14**
	8.2. Existen comités de seguridad de la información conformados en las entidades públicas	-	2	1	4	2	2	2	**13**
	8.3. No existe un nivel de avance del SGSI muy desarrollado en las entidades públicas	-	4	-	-	-	-	2	6
	8.4. La cultura organizacional del SGSI es poca o inexistente	**1**	**1**	**1**	**1**	**4**	**3**	**4**	**15**

Tabla N° 19 – **Relación entre los indicadores de la Organización del SGSI (Factor 8) y el número de incidencias presentadas en las entrevistas**

Factor Organización del SGSI	
Indicadores negativos - No se define un Alcance estándar en las entidades públicas - No existe un nivel de avance del SGSI muy desarrollado en las entidades públicas - La cultura organizacional del SGSI es poca o inexistente	**Indicadores positivos** - Existen comités de seguridad de la información conformados en las entidades públicas

Las conclusiones principales que se pudieron obtener en este punto es que no se tiene definido un alcance estandarizado institucional. La normativa de la NTP no precisa claramente qué tipo de Alcance del SGSI que debe ser definido en las organizaciones.

Por tanto, en el Alcance se puede especificar un área, un proceso, un sub-proceso o toda la institución y eso es justamente quizás uno de los errores más comunes que se está manejando. Tiene que haber un estudio preliminar para poder determinar el alcance real y que esto se alinee a los objetivos estratégicos que busca la

Organización pero esto debería ejecutarse en forma integral entre las instituciones públicas involucradas en la norma.

Es importante que se tenga un buen conocimiento de procesos para poder definir cómo un proceso se interrelaciona con otro, lo que finalmente determinará dicho Alcance. Por ende, debería existir un área de procesos en las organizaciones que le ayude al oficial de seguridad de información a determinar cuál es el mejor proceso de la organización para iniciar el SGSI.

Por otro lado, otro problema encontrado es que si bien existen en casi todas la instituciones entrevistadas comités de seguridad de información, se suele poner al oficial de seguridad como la persona que lidera el comité de seguridad de la información en la institución.

Sin embargo, el mayor obstáculo que se presenta en las entidades es la de crear conciencia al personal, cambiar los hábitos de trabajo, lo cual es difícil de modificar en las personas. Aún estamos tomando conciencia lentamente de la importancia de la seguridad de la información. En general no se capacita, no hay una cultura a nivel de las instituciones públicas de capacitar al personal, y no hay la cultura de invertir en capacitación.

Un factor restrictivo es principalmente la cultura organizacional respecto de la implementación del SGSI, lo cual es parte de un proceso de concientización de las personas que no están relacionadas con la norma. Es necesario para ello, mantener una coordinación muy extensa para las diferentes áreas de la organización entienda que la aplicación de la norma va más allá de lo tecnológico.

4.4.3. Discusión del análisis de datos

Los resultados obtenidos en este capítulo, se derivan de la evaluación realizada a las diferentes incidencias encontradas en cada uno de los factores establecidos en la investigación.

Por otro lado, en el Capítulo II de esta investigación (Marco Teórico), se han realizado un conjunto de investigaciones que recogen las principales causas que se presentan al implementar la seguridad de la información en las organizaciones públicas y privadas a nivel mundial.

En este apartado, se discuten los aspectos técnicos más relevantes respecto de los factores encontrados en las entrevistas realizadas en esta investigación comparándolos con los factores definidos en las investigaciones analizadas en el ítem 2.4.5. *(Investigación sobre los factores de seguridad de la información a nivel mundial).*

Desarrollo

1- Del análisis realizado en las entrevistas, se puede inferir que el principal problema que se presenta en la implementación de la seguridad de la información *a nivel estratégico* es la falta de atención de políticas integrales de Estado entre las entidades públicas, ya que si bien existe un organismo encargado (como es la ONGEI) que viene cumpliendo un papel normativo, no está haciendo un papel como ente implementador. Es necesario desarrollar un plan de seguridad nacional que permita optimizar el uso de recursos y unificación de esfuerzos interinstitucionales.

Algo muy importante de destacar y que se enfatizó en las entrevistas, fue la formalización del cargo del Oficial de Seguridad de la Información en la estructura

funcional de la organización y en los documentos de gestión institucional como son el ROF y MOF.

Finalmente, una de las recomendaciones fue la de aprovechar la experiencia obtenida por aquellas entidades que están más avanzadas en el SGSI, sobre todo en aquellas que ya han obtenido experiencia en la certificación, las cuales podrían extender sus conocimientos hacia otras entidades que aún están en las primeras etapas de la implementación.

Estas conclusiones obtenidas de las entrevistas pueden confirmarse con las investigaciones encontradas respecto del análisis de los factores de seguridad de la información a nivel mundial en el Capítulo II (2.4.5), donde, por ejemplo, en la investigación "*Política nacional de seguridad de la información: Un caso de estudio en Taiwán"* (Ku, 2009), se analiza cómo el gobierno de Taiwán viene impulsando fuertemente la política de seguridad nacional, cuya principal misión es promover y mejorar la implementación y certificación del SGSI a nivel nacional**.**

Además, el Gobierno también apoya la investigación académica, imparte cursos educativos y promueve la certificación profesional. De esta forma, más de 170 sectores públicos han acreditado la autenticación en SGSI.

Así también, el rango de clasificación de seguridad también se ha ampliado a casi 6,800 sectores públicos después de incluir las unidades educativas. El Centro Nacional de Operaciones de Seguridad (NSOC) también mejoró sus habilidades y proporciona protección de seguridad para las instituciones críticas durante todo el día.

En el estudio respecto de los *"Roles ejecutivos del comité de seguridad de la información"* (Williams, 2007), se hace una referencia de que existe un imperativo de seguridad de información, el cual es de suma importancia para el comercio

mundial. Dicha seguridad es un proceso continuo y donde el nivel de atención (que debe prestar el Estado) y el compromiso debieran seguir siendo una prioridad en todo momento. Por ello, es importante que se diseñe e implemente una estructura organizativa estratégica en seguridad de información de alto nivel.

En Canadá (*Boyli, 2013*), se ha realizado una agrupación de especialistas de operaciones de TI en un solo grupo de trabajo nacional. Además, se ha creado el Área de Servicios Compartidos, que es un nuevo departamento creado en el 2011 con más de 6,000 funcionarios que realizan los siguientes servicios:

1°) Consolidación de 485 Data Centers en solamente 07. 2°) Migración de todos los sistemas de correo electrónico a una sola plataforma. 3°) Creación de una única infraestructura de red de telecomunicaciones compartida.

Como podemos ver, estas políticas de estado estratégicas aplicadas en otros países debieran ser replicadas en forma similar en nuestro país, lo que conllevaría a una óptima implementación del SGSI en las Entidades Públicas del Estado Peruano.

2- Respecto del análisis de los factores que se han presentado en las entrevistas realizadas respecto de la implementación de la seguridad de la información *a nivel técnico,* se encuentran principalmente las de presupuesto y especialización en SGSI.

Un problema que se evidencia en todas las entrevistas realizadas, es la falta de un plan presupuestal para el SGSI. Esto se debe principalmente a que las entidades públicas no han tenido un conocimiento exacto de cómo implementar presupuestalmente la NTP relativa a la seguridad de la información. Incluso, muchas de ellas actualmente cubren las actividades del SGSI con presupuesto de otras áreas, principalmente del área de Tecnología de la Información.

Además, otro aspecto que no se tiene en cuenta, es que la implementación del SGSI en una organización no es solamente la inversión actual en el costo del proyecto, sino que también tiene un costo de mantenimiento en el tiempo. Esto demanda contar con un equipo de personas destinadas a tiempo completo a cumplir con actividades de gestión propias del SGSI, lo cual generalmente no se planifica a largo plazo.

Otro de los factores técnicos que se presenta es la falta de profesionales especializados en la implementación del SGSI, lo cual aún está en una etapa inicial. Por otro lado, normalmente el cargo de Oficial de Seguridad de la información (OSI) en las entidades públicas recae en un profesional sin la experiencia ni la capacitación necesaria en este tipo de tareas; y, teniendo en cuenta de que éste va a ser un interlocutor entre la Alta Dirección y las dependencias de la institución, es necesario contar con un staff de especialistas peruanos y extranjeros con conocimientos avanzados en este tema, los cuales no sólo tendrían como objetivo el monitoreo y avance de las entidades públicas, sino también la labor de formar especialistas certificados internacionalmente en seguridad de la información.

Estas conclusiones obtenidas de las entrevistas, han sido analizadas también en investigaciones respecto del análisis de los factores de seguridad de la información a nivel mundial en el Capítulo II (2.4.5), donde, por ejemplo, en la investigación "*factores que influyen en la gestión de seguridad de la información en empresas pequeñas y medianas de Turquía" (Yeniman, 2011)*, refiere que es importante contratar especialistas en seguridad de información en el staff de la empresa que formen al personal técnico y directivo, pudiendo ser incluso la contratación de servicios de consultoría inicialmente.

En otra investigación denominada: "*Política nacional de seguridad de la información: Un caso de estudio en Taiwán"* (Ku, 2009), hasta el momento, más de 3.700 sectores públicos han sido incluidos para salvaguardar sus sistemas de I&C. También se han llevado a cabo más de 50 cursos y conferencias de formación, en los que se capacitó a casi 20,000 trabajadores relacionados con la seguridad de información. Asimismo, más de 200 servidores han sido galardonados con el certificado profesional de seguridad de información y 32 organizaciones públicas y privadas han adquirido la certificación internacional para la seguridad de información.

En el estudio respecto de los *"Roles ejecutivos del comité de seguridad de la información"* (Williams, 2007), se analizaron una serie de factores a tener en cuenta, como son:

a) **El proceso de integración**, donde se ha estudiado que existe una creciente necesidad de integrar funciones anteriormente responsables de aspectos específicos de la seguridad en una entidad holística capaz de reconocer, prevenir y reaccionar ante cualquier amenaza a la información o a los activos dentro de una organización empresarial.
b) **Las responsabilidades de seguridad de la información** se da a todos los niveles de la organización, teniendo en cuenta que si bien los especialistas en seguridad tienen la responsabilidad de diseñar, implementar y gestionar las medidas de seguridad específicas que la entidad vaya a necesitar, en última instancia es responsabilidad de cada uno de los empleados ayudar a garantizar la seguridad de la información en las organizaciones.

3- Respecto de los factores que se presentan en la implementación de la seguridad de la información *a nivel operativo*, tenemos varios aspectos relacionados con la operatividad de la implementación del SGSI en las instituciones públicas. Es así que, respecto del factor de la gestión del SGSI, se puede concluir que las estrategias operativas de implementación de la NTP en las entidades son diversas, donde algunas están más desarrolladas que otras, no existiendo una política de gestión de conocimientos de aquellas entidades públicas que están más avanzadas.

Otro factor que influye es que generalmente se asocian las funciones de seguridad de información con el área de informática o que es una función de tecnologías de la información. Por ello, muchas entidades públicas limitan la seguridad de la información únicamente al área de informática. Esto trae aparejado que el personal de las demás áreas de la organización no se sienta involucrado con el SGSI.

Otro factor relevante que se ha encontrado es que las instituciones públicas son organizaciones funcionales y no están organizadas por procesos. Sin embargo, la NTP establece, como punto de partida, que la entidad organice sus actividades por procesos. Por tanto, una recomendación que se obtiene de las entrevistas es que se debería aplicar el ISO 9001 para asegurar la calidad de los procesos durante todo el ciclo de la norma. No es casualidad, por tanto, que las instituciones entrevistadas que se han certificado en SGSI, previamente habían aplicado la ISO 9001 como base para la implementación de la ISO 27001.

Finalmente, un factor de mucha relevancia para la implementación del SGSI es el de tener el apoyo de la Alta Dirección. En una de las entrevistas realizadas, un especialista refirió que para obtener el apoyo de la alta dirección en la institución y

se otorgue el respaldo necesario para el SGSI, ésta tiene que "comprarse" la idea de que la seguridad de la información es importante. Para ello, un punto primordial estratégico a resolver por el Estado es el de "vender" la seguridad de la información en las entidades públicas. Se recomienda, por tanto, establecer una estrategia de concienciación a todos los directivos de la Alta Dirección de las instituciones públicas explicándoles a detalle la importancia de la implementación del SGSI.

Otro factor restrictivo es principalmente la cultura organizacional respecto de la implementación del SGSI, lo cual es parte de un proceso de concientización de las personas que no están relacionadas con la norma. El mayor obstáculo que se presenta en las entidades es la de crear conciencia al personal, cambiar los hábitos de trabajo, lo cual es difícil de modificar en las personas. Aún estamos tomando conciencia lentamente de la importancia de la seguridad de la información. En general no se capacita, no hay una cultura a nivel de las instituciones públicas de capacitar al personal, y no hay la cultura de invertir en capacitación.

Estas conclusiones obtenidas de las entrevistas, han sido analizadas también en investigaciones respecto del análisis de los factores de seguridad de la información a nivel mundial en el Capítulo II (2.4.5), donde, por ejemplo, en la investigación "*factores que influyen en la gestión de seguridad de la información en empresas pequeñas y medianas de Turquía" (Yeniman, 2011)*, refiere entre sus conclusiones que son factores importantes el apoyo que brindan, tanto la Alta Dirección como los empleados, a las políticas de seguridad de información institucional, así como también la obligación de todas las personas y empresas a cooperar en la conformación de dichas políticas.

Otra investigación denominada *"Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad financiera de segundo piso"* (Guzman, 2015), permitió conocer, por referencias de los directivos de la entidad, que debido a la experiencia en la ejecución de la ISO 9001, se ha logrado una clara comprensión de la implementación de un sistema de gestión en la organización. Cuando se comenzó la implementación del SGSI, esta entidad encontró, por ejemplo, que el concepto de control de seguridad ya se había incorporado en muchas operaciones y procesos internos cuando se implementó la ISO 9001.

Esta investigación permitió encontrar otros factores que han influido en la implementación del SGSI en esta organización, tales como:

a) La experiencia pasada de otras normas ISO

Con la experiencia pasada de la ISO 9001, el personal de esta organización ya estaba preparado para afrontar la ejecución del SGSI bajo la ISO 27001, debido a que la arquitectura y los procesos de aplicación de las normas 9001 y 27001 son consistentes.

b) La cultura de la organización

La cultura de seguridad de la información de una organización puede ser un factor importante para el mantenimiento de un nivel adecuado de seguridad de la información en esa organización. (Von Solms, 2000).

De acuerdo a los resultados de esta investigación, esta institución es agresiva en la adopción de nuevos sistemas tecnológicos y de gestión debido a su cultura organizacional, la cual es de una alta calidad; por lo que no es de extrañar que sea fácil y natural promover la implementación del SGSI en esta organización. Los resultados de este estudio indican que la experiencia pasada con éxito en otras normas, la disponibilidad de los documentos

necesarios, el aprendizaje y la cultura organizacional son las principales motivaciones de una implementación exitosa del SGSI en una organización.

En otro estudio denominado “Los 10 pecados capitales de la gestión de la seguridad de la información” (Von Solms, 2004), se identificaron aspectos esenciales, los cuales según el autor, si no son tomados en cuenta en un plan de gobierno de la seguridad de la información, harán que dicho plan fracase o al menos causen graves fallas en el mismo.

Entre algunos de estos factores tenemos los siguientes:

- Es esencial que una empresa deba contar con una estructura organizativa de seguridad de la información adecuada para hacer un plan de seguridad de la información exitoso. Esta estructura tiene que ver con la forma en que está organizada una empresa en seguridad de la información con códigos de buenas prácticas de seguridad.
- En otros casos, la dirección ejecutiva en las empresas todavía piensa que la tecnología es todo lo que se requiere, y por lo tanto, se delega a los departamentos técnicos, y paulatinamente se olvidan de él. Las consecuencias de ello es que el problema de seguridad de la información será enfocada en la tecnología únicamente, en lugar de una solución total integral.
- Así también, no existen programas de sensibilización adecuados, y los usuarios no son conscientes de los riesgos del uso de la infraestructura informática de la empresa, y los posibles daños que pueden causar. Por otra parte, a menudo ni siquiera son conscientes de las políticas, procedimientos y normas de seguridad de la información existentes en la empresa.

CAPITULO 5 – CONCLUSIONES Y RECOMENDACIONES

El Estado Peruano, a través de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI - de la Presidencia del Consejo de Ministros, como ente rector de la implementación de la Política Nacional de Gobierno Electrónico, desde su creación ha emitido normas, en forma orgánica y sistematizada, con el fin de desarrollar la Seguridad de la Información de acuerdo a estándares internacionales. Sin embargo, existen factores que restringen o impiden el avance y ejecución del proceso de implementación del Sistema de Gestión de Seguridad de la Información en el sector público.

Todo esto se puede evidenciar revisando los indicadores de la VIII Encuesta Nacional de Recursos Informáticos en la Administración Pública (ENRIAP- Pág. 75) llevada a cabo por la ONGEI, donde se indica que, de 552 entidades del sector público encuestadas, solamente 182 de ellas (33%) ha iniciado el proceso de implementación del SGSI basadas en la NTP-ISO/IEC 17799 (Norma anterior vigente del SGSI antes de la NTP-ISO/IEC 27001).

Por otro lado, según un estudio respecto del nivel de maduración de la Seguridad de Información en el Perú (realizado por la empresa JackSecurity), se concluye que el Gobierno de la Seguridad de la Información se encuentra en un nivel de maduración “informal” (de nivel 2, según modelo de maduración ITGI de 0 a 5).

Por tanto, se hace necesario establecer estrategias, respecto de la implementación del SGSI en la Administración Pública Peruana basadas en la NTP-ISO/IEC 27001, que estén más orientadas a dotar de una estructura organizacional de gestión de la información que permita el alineamiento de TI con la estrategia de negocios de las organizaciones, el logro de beneficios, la reducción de costos, el control de riesgos y en general la mejora de las operaciones de TI en las organizaciones.

El propósito de este estudio es realizar una investigación de tipo cualitativa que nos ha permitido utilizar una metodología de recopilación de información de una manera organizada y estructurada, a través de la realización de entrevistas, para identificar las restricciones y facilidades que encuentran las entidades públicas, donde se han establecido un conjunto de variables de estudio para obtener información de apoyo a la mejora de las políticas de seguridad de información de las entidades integrantes del Sistema Nacional de Informática del Sector Público, de tal manera de poder encontrar un punto de equilibrio entre el alineamiento de TI con la estrategia de negocio de la organización y el control de riesgos de seguridad de la información, que faciliten la evaluación del nivel de complejidad de los factores que no permiten el desarrollo de la implementación integral de la NTP-ISO/IEC 27001.

Para el desarrollo de esta investigación, se concretaron 07 entrevistas semiestructuradas con las siguientes instituciones públicas: Ministerio de Relaciones Exteriores - RR.EE., Registro Nacional de Identificación y Estado Civil - RENIEC, Instituto del Mar del Perú - IMARPE, Oficina Nacional de Procesos Electorales - ONPE, el Ministerio Público - Fiscalía de la Nación - MPFN, el Ministerio de Economía y Finanzas - MEF y el Ministerio de Cultura - CULTURA.

Considero que las entrevistas realizadas son suficientes para responder la pregunta de investigación de la presente tesis.

La investigación realizada tiene las siguientes características:

Por su estrategia técnico-metodológica, *la investigación es cualitativa* porque pretende identificar los factores que restringen la implementación del Sistema Gestión de Seguridad de la Información en las Entidades de la Administración Pública según la NTP-ISO/IEC 27001.

Por su finalidad, *la investigación es básica* porque pretende desarrollar una teoría respecto de las facilidades y restricciones para la implementación de la NTP 27001 dentro de las instituciones del Estado.

Por los objetivos, *la investigación es descriptiva* porque pretende identificar todos aquellos aspectos que afectan el desarrollo del proceso de implementación del Sistema Gestión de Seguridad de la Información en las Entidades Públicas.

Por los tipos de datos que se trabajarán, *éstos serán Primarios* porque para identificar los factores que restringen la implementación del Sistema Gestión de Seguridad de la Información se realizaron entrevistas que permitirán levantar información de primera mano.

Por el grado de control, *la investigación es no experimental* porque no podríamos controlar todas las variables identificadas.

Por la secuencia temporal, *la investigación es transversal* porque no se realizará el método de investigación en distintos momentos para ver su evolución, sino que se realizará en un solo periodo de tiempo.

5.1. CONCLUSIONES

Las conclusiones a las que se ha podido llegar al finalizar todas las etapas de la investigación responden a la pregunta de la investigación: ***¿Cuáles son los factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas Peruanas según la NTP-ISO/IEC 27001?***, y son las siguientes:

El desarrollo de la investigación nos ha permitido encontrar ocho categorías que representan los factores que afectan la implementación del SGSI en las entidades públicas peruanas. Estos elementos han sido distribuidos en 03 niveles:

I) Nivel Estratégico

1.1- Una Política Estratégica de Estado en Seguridad de la Información

II) Nivel Operativo: 04 pilares operacionales

2.1- Una gestión eficiente de la seguridad de información,

2.2- Apoyo institucional de la Alta Dirección

2.3- Una adecuada organización del SGSI

2.4- Aplicación efectiva de la normatividad en seguridad de información

III) Nivel Técnico: Compuesta de 03 partes

3.1- Desarrollo integral institucional de la NTP

3.2- Contar con un presupuesto nacional para la seguridad de la información

3.3- La especialización técnica de profesionales en SGSI como prioridad nacional

Esta representación, nos permite definir las siguientes aseveraciones:

- El factor más importante a tener en cuenta es impulsar desde el Gobierno Central, una Política Estratégica de Estado que conlleve a formalizar

funcionalmente el cargo de Oficial de Seguridad de Información en la estructura orgánica de las entidades del sector público a través de los instrumentos de gestión institucional vigentes como son el ROF y el MOF. El diseño de esta Política es necesaria para el establecimiento operativo sobre la que se soportará la misma.

Esto conlleva a la necesidad de establecer la creación de un Departamento de Gobierno de Seguridad de la Información -del más alto nivel- compuesto por un grupo de especialistas en seguridad de la información que opere como un solo grupo de trabajo nacional el cual tenga como principal función un monitoreo permanente de avance y ejecución del avance de la implementación del SGSI en todas las entidades públicas peruanas, lo que podría darse a través de la potenciación funcional y técnica de la ONGEI.

- Actualmente, las entidades -tanto públicas como privadas- vienen enfrentando desafíos, en este ámbito, los cuales se han tornado más sofisticados y pueden llegar a ser potencialmente devastadores. Por ello, esta política estratégica debe incluir un acompañamiento en la gestión y la definición de sus procesos en cada una de las organizaciones involucradas.

  Del análisis realizado en las entrevistas a las entidades públicas que ya se han certificado en ISO 27001, se ha visto que una de las estrategias utilizadas ha sido el iniciar con la identificación y ordenamiento de sus procesos a través de la ISO 9001 como soporte de gestión por procesos. Estas instituciones han confirmado que para completar las fases de implementación del SGSI, es muy importante tener claros los procesos de negocio de la institución.

- Otro elemento a tener en cuenta es el presupuestal, de tal manera de contar con los recursos financieros para llevar a cabo dicha implementación que sea

administrada por una entidad central como la Oficina Nacional de Gobierno Electrónico (ONGEI), que asumiría un rol más proactivo en la ejecución de la Política Estratégica de Seguridad de la Información.

- Por último, no hay que perder de vista el factor de profesionalización de especialistas en seguridad de información en el Estado, la que actualmente es escasa y que es necesario darle un mayor recurso técnico para una eficiente ejecución operativa.

- Otros aspectos destacados de esta investigación son:
  - El 100% de las entidades públicas entrevistadas dispone de un área específica para la seguridad de la información, si bien está integrada mayoritariamente en el departamento de TI (70%).
  - La figura del Oficial de Seguridad de la Información aún está en implementación en las organizaciones públicas peruanas y la seguridad de la información recae principalmente en un responsable integrado dentro del departamento de TI.
  - Existe una gran sensibilidad hacia los temas de seguridad de la información por parte de los Oficiales de Seguridad de la Información de las Organizaciones Estatales. En particular, la mayoría de los entrevistados de esta investigación aseguran tener una certificación ISO 27001, CISA, CISM, CRISC y PMI.
  - Los principales factores de preocupación en el ámbito de la seguridad de la información son las regulaciones y las normativas de ejecución obligatoria en este ámbito. Por ello, se establece necesario no sólo un gasto eficiente de los presupuestos sino también el despliegue eficiente de los mismos.

En base a todo lo referido anteriormente, se ha elaborado un diagrama que permite visualizar gráficamente las conclusiones obtenidas.

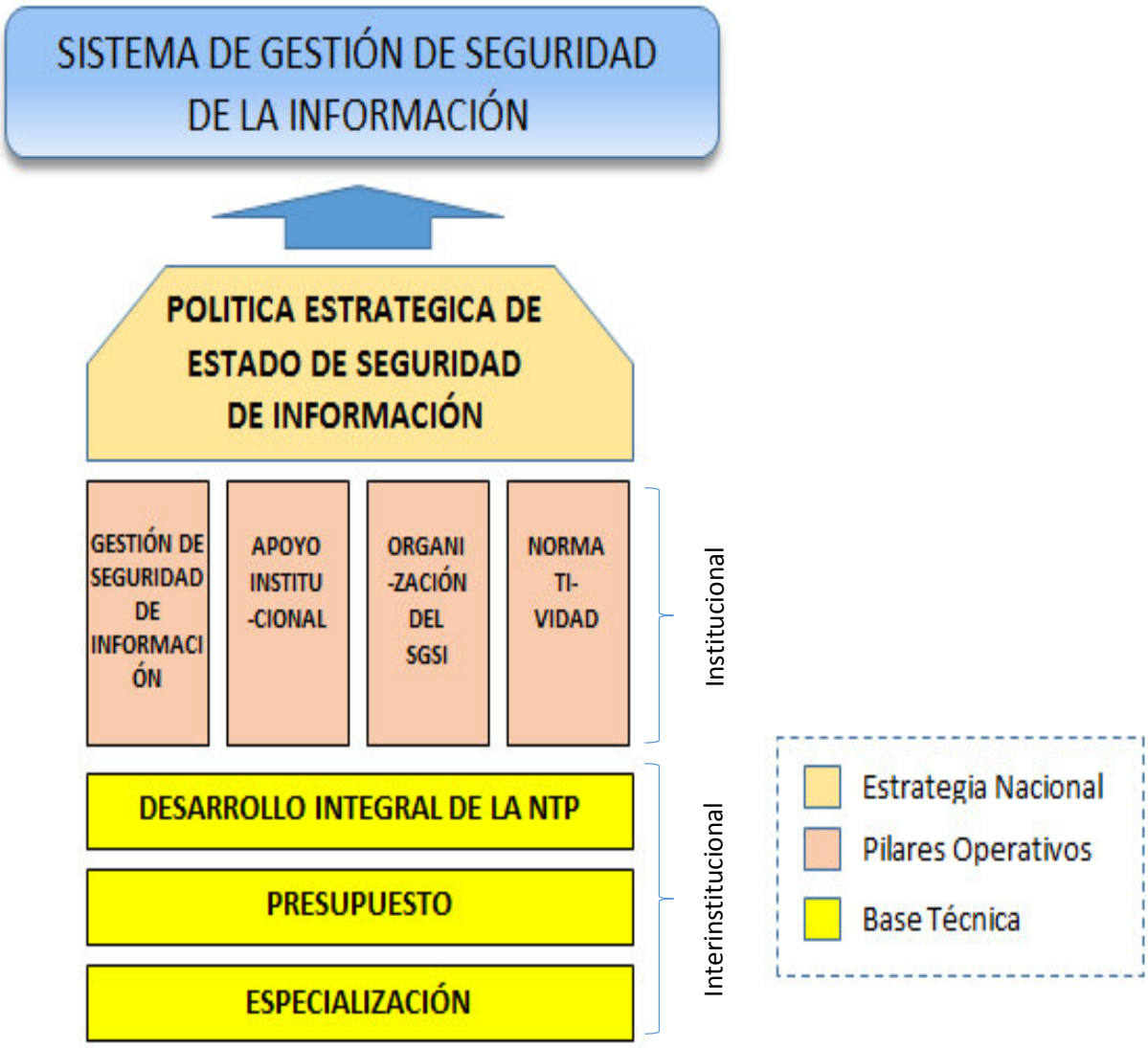


Gráfico N° 20: **Diagrama de factores que afectan la implementación del SGSI en las Entidades Públicas Peruanas**

5.2. RECOMENDACIONES

El presente estudio de investigación recomienda lo siguiente:

- Se requerirá el establecimiento de una norma para la creación de un Departamento de Gobierno de SGSI, que tendrá como objetivo:

  a. Establecer políticas estandarizadas de Seguridad de la Información
  b. Diseñar y armonizar normativas institucionales en materia de Seguridad de la Información
  c. Facilitar la incorporación de todos los entes gubernamentales a la Seguridad de la Información
  d. Brindar instrumentos a las instituciones gubernamentales para la implementación del SGSI en el gobierno

  Este Departamento deberá ser adscrito a la ONGEI o a la PCM, y deberá contar con capacidad funcional para operar a nivel de todo el Estado.

- Apoyarse en las certificaciones como mecanismo para asegurar el correcto funcionamiento del Sistema de Gestión de la Seguridad de la Información, del Plan de Continuidad de Negocio y del Plan de Contingencia Tecnológica.

- Aplicar estrategias para la concientización del personal en seguridad de la información, a través de la ejecución de un plan operativo de concientización y capacitación -incluido en los documentos de gestión de la organización- mediante la evaluación de la gestión del conocimiento utilizando estándares de TI.

- Es necesario asignar un presupuesto central para una gestión adecuada de los recursos de seguridad de la información en la implementación del SGSI en las entidades del Estado Peruano según lo dispuesto en la NTP-ISO/IEC 27001.

5.3. FUTURAS INVESTIGACIONES

El presente estudio de investigación ha identificado los factores que restringen o impiden el avance y ejecución del proceso de implementación del Sistema de Gestión de Seguridad de la Información basada en la NTP-ISO/IEC 27001, en las Entidades Públicas Peruanas. Así también, ha permitido establecer una categorización de estos factores en 03 niveles de gestión con una visión holística e integral del gobierno de seguridad de la información.

Por todo esto, se plantean los siguientes estudios futuros que complementarían la presente investigación, como son:

- Una investigación respecto de la implementación de la NTP de Seguridad de la Información en el Estado Peruano, aplicando la metodología de Gobierno de Seguridad de la Información (ISO 27014), que permita identificar las características principales de los factores estratégicos, técnicos y operativos que influyen en la gestión integral del SGSI.
- Un estudio técnico sobre un modelo de implementación del Sistema de Gestión de Seguridad de la Información en las entidades públicas integrando la gestión por procesos bajo la norma ISO 9001, que permita comprender la estructura operativa y los principales actores de las organizaciones relacionadas con la seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

[1] Asociación Colombiana de Ingenieros de Sistemas-ACIS. (2012). IV Encuesta Latinoamericana de Seguridad de la Información 2012. Recuperado el 15 de enero de 2014 desde http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-no-123/item/101-iv-encuesta-latinoamericana-de-seguridad-de-la-información

[2] Ayala, L. Hernández, R. Revelo, L. Solarte, F. (2012). Diagnóstico del Estado de los Sistemas de Gestión de Seguridad de la Información en Instituciones de Educación Superior de San Juan de Pasto. En Universidad Nacional Abierta y a Distancia UNAD, I Congreso Nacional e Internacional de Innovación, Investigación y Competitividad frente al TLC, (pp. 302-325). Nariño, Colombia. Recuperado el 20 de diciembre de 2013 desde http://www.iucesmag.edu.co/editorial/files/la_investigacion_como_aporte_al_emprendimiento_y_la_innovacion.pdf

[3] Bhaskar, R. Kapoor, B. (2013). Chapter 3 – Information Technology Security Management. *Managing Information Security (Second Edition), p57-74.* Recuperado el 09 de diciembre de 2013 desde http://www.sciencedirect.com/science/article/pii/B9780124166882000039

[4] Bojanc, R. Jerman-Blažič, B. Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing & Management, 48(6), p1031-1052.* Recuperado el 09 de diciembre de 2013 desde http://www.sciencedirect.com/science/article/pii/S0306457312000027

[5] Boyli, B. (2013). La Seguridad de la Información en el Gobierno de Canadá. En Colegio de Ingenieros del Perú. 54. Lima, Perú. Recuperado el 09 de diciembre de 2013 desde http://www.cip.org.pe/index.php/eventos/conferencias-ceremonias-y-patrocinios/item/572-la-seguridad-de-la-informacion-en-el-gobierno-de-canada/572-la-seguridad-de-la-informacion-en-el-gobierno-de-canada.html

[6] Brewster, B. Jahangri, N. Hassanzadeh, M. (2013). Chapter 6 – A Conceptual Framework for Information Security Awareness, Assessment, and Training. *Emerging Trends in IT Security, p99-100.* Recuperado el 04 de febrero de 2014 desde http://www.sciencedirect.com/science/article/pii/B9780124114746000062

[7] BuenasTareas.com. (2012). SGSI - Modelos de Maduración. Recuperado el 06 de diciembre de 2013 desde https://www.buenastareas.com/ensayos/Sgsi-Modelo-de-Maduracion/3951245.html

[8] Cao Avellaneda, J. (2011). Medición de un SGSI: Diseñando el Cuadro de Mandos (I). Recuperado el 06 de diciembre de 2013 desde https://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Medicion_de_un_SGSI_disenando_el_cuadro_de_mandos_I

[9] Cao Avellaneda, J. (2011). Medición de un SGSI: Diseñando el Cuadro de Mandos (II). Recuperado el 06 de diciembre de 2013 desde

https://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Medicion_de_un_SGSI_disenando_el_cuadro_de_mandos_II

[10] Carrillo, J. Rubio, P. (2011). Modelo de Procesos Integrado de Gobernanza y Gestión de TI. *AEMES, pp.29-45.* Facultad de Informática, Universidad Politécnica de Madrid, España.

[11] Consejo Nacional de la Competitividad - CNC. (2015). Análisis de la normatividad en TIC y recomendaciones de mejora. Iriarte y Asociados S.CIVL de R.L. desde

http://www.cnc.gob.pe/images/upload/paginaweb/archivo/25/An%C3%A1lisis%20de%20la%20Normatividad%20TIC.pdf

[12] Cuñat, R.J. (2005). Aplicación de la teoría fundamentada al estudio del proceso de creación de empresas. *Decisiones Globales*, *pp. 1-13*.

[13] Da Veiga, A. Eloff, J.H.P. (2010). A framework and assessment instrument for information security culture. *Computer&Security, 29(2), p196-207.* Recuperado el 05 de febrero de 2014 desde http://www.sciencedirect.com/science/article/pii/S0167404809000923

[14] Dzazali, S. Sulaiman, A. Zolait, A. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Goverment Information Quaterly, 26(4), p584-593.* Recuperado el 09 de diciembre de 2013 desde http://www.sciencedirect.com/science/article/pii/S0740624X09000859

[15] Ernst & Young. (2013). En la lucha por cerrar la brecha. *XV Encuesta Global de Seguridad de la Información.* Recuperado el 02 de febrero de 2014 desde

http://www.ey.com/Publication/vwLUAssets/XV_Encuesta_Global_Seguridad_de_la_Informacion/$FILE/XV_Encuesta_Global_de_Seguridad_Informacion.pdf

[16] Ernst & Young. (2012). Salir de la niebla para entrar en la nube. *XIV Encuesta Global de Seguridad de la Información.* Recuperado el 02 de febrero de 2014 desde

http://www.ey.com/Publication/vwLUAssets/Salir_de_la_niebla_para_entrar_a_la_nube/$FILE/XIV_EGSI_Salir_niebla_%20para_entrar_nube.pdf

[17] Ernst & Young. (2011). Seguridad sin fronteras. *XIII Encuesta Global de Seguridad de la Información.* Recuperado el 03 de febrero de 2014 desde

http://www.ey.com/Publication/vwLUAssets/Presentacion_ejecutivo_del_evento_Seguridad_al_dia/$FILE/Presentacion_resultados_13EGSI.pdf

[18] Fernández, C. (2012). La norma ISO 27001 del Sistema de gestión de Seguridad de la Información. *Seguridad y Salud*, pp. 43-44.

[19] Frankland, Jane. (2008). Métricas de Seguridad de TI: Implementación y cumplimiento de estándares. *Network Security, 2008(6), p6-9.* Recuperado el 10 de diciembre de 2013 desde http://www.sciencedirect.com/science/article/pii/S1353485808700758

[20] Gil, Jorge A. (2011). Gobierno de TI. *Sistemas, 118(2), p82-87.* Recuperado el 10 de enero de 2014 desde http://www.acis.org.co/fileadmin/Revista_118/Cuatro.pdf

[21] Guerra, M. Jordan, V. (2010). Políticas Públicas de la Sociedad de la Información en América Latina ¿Una misma visión? En CEPAL (Ed.). Recuperado el 02 de febrero de 2014 desde http://repositorio.cepal.org/bitstream/handle/11362/3757/S2010178.pdf?sequence=1

[22] Guzman, C. (2015). *Diseño de un sistema de gestión de la seguridad de la información para una entidad financiera de segundo piso.* Institución Universitaria Politécnico Grancolombiano. Facultad de Ingeniería y Ciencias Básicas. Especialización en Seguridad de la Información. Bogotá, Colombia. Recuperado el 31 de marzo de 2016 desde http://repository.poligran.edu.co/bitstream/10823/746/1/Proyecto de Grado SGSI - IGM- CarlosGuzman (FINAL).pdf

[23] IDC España. (2012). Análisis de la Seguridad de la Información en España desde http://necsia.es/wp-content/uploads/2012/07/Resumen-Ejecutivo-Seguridad-de-la-Informaci%C3%B3n-NECSIAcalidad-env%C3%ADo.pdf

[24] INDECOPI. (2009). Norma Técnica Peruana NTP-ISO/IEC 27001:2008. EDI. Tecnologías de la información. Sistemas de Gestión de Seguridad de la Información. Requisitos. Recuperado el 10 de enero de 2014 desde http://bvirtual.indecopi.gob.pe/normas/isoiec27001.pdf

[25] JackSecurity. (2008). Gobierno de Seguridad de la Información. Nivel de Maduración – Perú 2008. Recuperado el 11 de enero de 2014 desde http://www.jacksecurity.com/download.php?idP=82&ida=83

[26] Knapp, K. Morris, F. Marshall, T. (2009). Information security policy: An organizational-level process model. *Computers & Security, Volume 28, Issue 7. Pages 493-508.* Recuperado el 28 de Marzo de 2016 desde http://www.sciencedirect.com/science/article/pii/S0167404809000765

[27] KPMG. (2012). Informe de fraude en el Perú 2012. Recuperado el 02 de febrero de 2014 desde

http://www.kpmg.com/PE/es/IssuesAndInsights/ArticlesPublications/Documents/Informe-del-Fraude-en-Peru-2012.pdf

[28] Krishna, K. (2011). ISACA Journal. *Information Security Management for Governments.* Volume 4, p1-5.

[29] Ku, Ch. Chang, Y. Yen, D. (2009). National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy, 33(7), p371-384.* Recuperado el 13 de diciembre de 2013 desde http://www.sciencedirect.com/science/article/pii/S0308596109000263

[30] Larrondo, A. (2010). *Uso de la Norma ISO/IEC 27004 para Auditoría Informática.* Universidad Carlos III de Madrid, España. Recuperado el 17 de diciembre de 2013 desde http://orff.uc3m.es/bitstream/handle/10016/10564/PFC_agustin_Larrondo_Quiros.pdf?sequence=1

[31] Mariño, A. (2010). *Factores inhibidores en la implementación de sistemas de gestión de la seguridad de la información basados en la NTP-ISO/IEC 17799 en la administración pública.* Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería de Sistemas. Lima, Perú. Recuperado el 30 de noviembre de 2013 desde http://cybertesis.unmsm.edu.pe/handle/cybertesis/1058

[32] Matas Terrón, A. (2010). Computadoras e investigación cualitativa. AIDESOC. Recuperado desde http://riuma.uma.es/xmlui/bitstream/handle/10630/4712/computadoras_inves_cualitativa.pdf?sequence=1

[33] Ministerio de Ambiente, Energía y Telecomunicaciones. (2011). Estado de Seguridad Informática en el Sector Público Costarricense. Costa Rica: MINAET. Recuperado el 30 de noviembre de 2013 desde

http://www.telecom.go.cr/index.php/publicaciones/telecom/publicaciones/estado-de-la-seguridad-informatica-en-el-sector-publico/download.

[34] Ormella, C. (2011). *Métricas de Seguridad de la Información y Gestión del Desempeño con el Balanced ScoreCard***.** Recuperado el 02 de diciembre de 2013 desde http://www.iso27000.es/download/Carlos_Ormella-metricas_segu_info_bsc.pdf

[35] Ormella, Carlos (2013). *Cómo medir la efectividad de la Concientización*. Recuperado el 03 de diciembre de 2013 desde http://www.criptored.upm.es/descarga/metricas_efectividad_conciencia.pdf

[36] Pallas, G. (2009). *Metodología de implantación de un SGSI en un grupo empresarial jerárquico.* Universidad de la República. Instituto de Computación - Facultad de Ingeniería. Montevideo, Uruguay. Recuperado el 01 de diciembre de 2013 desde http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

[37] Pereyro, Maria. (2011). Seguridad de la información en el Uruguay: políticas de Estado en la Administración Pública. *Revista de la Asociación de Escribanos del Uruguay, Tomo 97.* Recuperado el 03 de enero de 2014 desde http://documentos.aeu.org.uy/090/097-1-137-156.pdf

[38] Presidencia del Consejo de Ministros-ONGEI (Ed). (2013). 10 años de Gobierno Electrónico en el Perú. *Seguridad de la Información: Una mirada al Gobierno Electrónico en el Perú (pp.65-66). Lima: ONGEI.*

[39] Presidencia del Consejo de Ministros -ONGEI. (2012). Resolución Ministerial N° 129-2012-PCM. Aprobación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información.

[40] Presidencia del Consejo de Ministros-ONGEI. (2012). Resolución N° 084-2012/CNB-INDECOPI. Aprobación de la Norma Técnica Peruana NTP-ISO/IEC 27004:2012. Técnicas de Seguridad. Gestión de Seguridad de la Información. Medición. Recuperado el 16 de diciembre de 2013 desde http://www.mef.gob.pe/contenidos/servicios_web/conectamef/pdf/normas_legales_2012/NL20121012.pdf

[41] Presidencia del Consejo de Ministros-ONGEI. (2010). Resolución Ministerial N° 187-2010-PCM. Autorización para la ejecución de la "Encuesta de Seguridad de la Información en la Administración Pública - 2010".

[42] Presidencia del Consejo de Ministros-ONGEI. (2013). La Seguridad de la Información en el Gobierno Peruano. En Colegio de Ingenieros del Perú. Lima, Perú. Recuperado el 09 de diciembre de 2013 desde http://www.cip.org.pe/index.php/eventos/conferencias-ceremonias-y-patrocinios/item/572-la-seguridad-de-la-informacion-en-el-gobierno-de-canada/572-la-seguridad-de-la-informacion-en-el-gobierno-de-canada.html

[43] Presidencia del Consejo de Ministros-ONGEI. (2013). Resolución Ministerial N° 310-2013-PCM. Autorización para la ejecución de la "Encuesta Nacional de Recursos Informáticos en la Administración Pública - ENRIAP".

[44] Presidencia del Consejo de Ministros-ONGEI. (2010). Análisis Encuesta Nacional de Recursos Informáticos y Tecnológicos de la Administración Pública - VIII ENRIAP. Recuperado el 11 de enero de 2014 desde http://www.ongei.gob.pe/publica/indicadores/Analisis_Encuesta_VIII_ENRIAP_2010.pdf

[45] Rayme, R. (2007). *Gestión de la Seguridad de la Información y los servicios críticos de la Universidad: Un estudio de 3 casos en Lima Metropolitana.* Universidad Nacional Mayor de San Marcos. Facultad de Ciencias Administrativas. Lima, Perú. Recuperado el 13 de febrero de 2014 desde http://cybertesis.unmsm.edu.pe/xmlui/handle/cybertesis/428

[46] Santos-Olmo, A. Sánchez, L.E. Villafranca, D. Fernández-Medina, E. (2011). SCMM - PYME: Modelo de Madurez de la Seguridad para Pymes. En Asamblea General de la Plataforma Tecnológica Española de Tecnologías de Seguridad y Confianza. Bucaramanga, Colombia. Recuperado el 02 de diciembre de 2013 desde http://www.ametic.es/CLI_AETIC/ftpportalweb/documentos/daniel_villafranca_sicaman.pdf

[47] Santos-Olmo, A. Sánchez, L.E. Fernández-Medina, E. Piattini, M. (2012). Métricas de Seguridad en los SGSI, para conocer el nivel de seguridad de los SS.OO. y de los SGBD. *Puente*, *6(1), p31-41.* Recuperado el 06 de diciembre de 2013 desde http://puente.upbbga.edu.co/index.php/revistapuente/article/view/68

[48] Talabis, M. Martin, J. (2012). Chapter 1 – Information Security Risk Assessments. *Information Security Risk Assessments, p1-26*. Recuperado el 15 de diciembre de 2013 desde http://www.sciencedirect.com/science/article/pii/B9781597497350000014

[49] Talabis, M. Martin, J. (2012). Chapter 2 – Information Security Risk Assessment: A Practical Approach. Information Security Risk Assessments, p27-62. Recuperado el 15 de diciembre de 2013 desde http://www.sciencedirect.com/science/article/pii/B9781597497350000026

[50] Talabis, M. Martin, J. (2012). Chapter 3 – Information Security Risk Assessment: Data Collection. Information Security Risk Assessments, p63-104. Recuperado el 15 de diciembre de 2013 desde http://www.sciencedirect.com/science/article/pii/B9781597497350000038

[51] Tena, A. (2010). *Cap 14 - Recolección y análisis de los datos cualitativos*. El proceso de la investigación cualitativa, p.581 – 683. Dpto Psicología. Universidad Iberoamericana. México. Recuperado desde http://drtoro-psyc608.wikispaces.com/file/view/Cap%C3%ADtulo+14.pdf

[52] Villafranca, D. Fernandez-Medina, E. Piattini, M. (2011). Definición de un modelo automatizado para la evaluación y mantenimiento de un SGSI. En Universidad de Castilla-La Mancha, España. V Congreso Iberoamericano de Seguridad Informática, CIBSI 2011. Bucaramanga, Colombia.

[53] Villafranca, D. Sanchez, L.E. Fernandez-Medina, E. Piattini, M. (2009). Metodología para la selección de métricas en la construcción de un Cuadro de Mando Integral. En Universidad de Castilla-La Mancha, España. III Congreso Iberoamericano de Seguridad Informática, CIBSI 2009. Bucaramanga, Colombia. Recuperado el 30 de noviembre de 2013 desde http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3(5).pdf

[54] Von Solms, B. Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, Volume 23, Issue 5. Pages 371-376.* Recuperado el 21 de Marzo de 2016 desde http://www.sciencedirect.com/science/article/pii/S0167404804001221

[55] Williams, P. (2007). Executive and board roles in information security. *Network Security, Volume 2007, Issue 8. Pages 11-14.* Recuperado el 23 de Marzo de 2016 desde http://www.sciencedirect.com/science/article/pii/S1353485807700739

[56] Yeniman, E. Akalp, G. Aytac, S. Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management, Volume 31, Issue 4. Pages 360-365.* Recuperado el 23 de Marzo de 2016 desde http://www.sciencedirect.com/science/article/pii/S0268401210001520

ANEXOS

ANEXO 1: FORMATO DE CONSENTIMIENTO INFORMADO (Presentación) PARA LOS PARTICIPANTES DE LA INVESTIGACIÓN

El propósito de esta ficha de consentimiento es proveer a los participantes en esta investigación con una clara explicación de la naturaleza de la misma, así como de su rol en ella como participantes.

La presente investigación es conducida por Javier Alfonso Seclén Arana, estudiante de Postgrado de la Universidad Nacional Mayor de San Marcos – UNMSM. La investigación tiene como propósito realizar un estudio que recoja de manera organizada y estructurada las restricciones que encuentran las gerencias de informática de las entidades del Sistema Nacional de Informática en el Perú para la implementación del Sistema de Gestión de Seguridad de la Información según la NTP-ISO/IEC 27001.

Si usted accede a participar en este estudio, se le pedirá responder preguntas en una entrevista. Esto tomará aproximadamente sesenta (60) minutos de su tiempo. Lo que conversemos durante estas sesiones se grabará, de modo que el investigador pueda transcribir después las ideas que usted haya expresado.

La participación es este estudio es estrictamente voluntaria. La información que se recoja será confidencial y no se usará para ningún otro propósito fuera de los de esta investigación. Sus respuestas al cuestionario y a la entrevista serán codificadas usando un número de identificación y por lo tanto, serán anónimas. Una vez trascritas las entrevistas, los cassettes (o cualquier otro instrumento utilizado) con las grabaciones se destruirán.

Si tiene alguna duda sobre este proyecto, puede hacer preguntas en cualquier momento durante su participación en él. Igualmente, puede retirarse del proyecto en cualquier momento sin que eso lo perjudique en ninguna forma. Si alguna de las preguntas durante la entrevista le parecen incómodas, tiene usted el derecho de hacérselo saber al investigador o de no responderlas.

Desde ya se le agradece su participación.

_____

Javier A. Seclén Arana

DNI N°

ANEXO 1: FORMATO DE CONSENTIMIENTO INFORMADO (Entrevistado) PARA LOS PARTICIPANTES DE LA INVESTIGACIÓN

Acepto participar voluntariamente en esta investigación, conducida por Javier Alfonso Seclén Arana. He sido informado (a) de que la meta de este estudio tiene como propósito realizar un estudio que recoja de manera organizada y estructurada las restricciones que encuentran las gerencias de Informática de las entidades del Sistema Nacional de Informática en el Perú para la implementación del Sistema de Gestión de Seguridad de la Información según la NTP-ISO/IEC 27001.

Me han indicado también que tendré que responder cuestionarios y preguntas en una entrevista, lo cual tomará aproximadamente sesenta (60) minutos.

Reconozco que la información que yo provea en el curso de esta investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de este estudio sin mi consentimiento. He sido informado de que puedo hacer preguntas sobre el proyecto en cualquier momento y que puedo retirarme del mismo cuando así lo decida, sin que esto acarree perjuicio alguno para mi persona. De tener preguntas sobre mi participación en este estudio, puedo contactar al responsable de la investigación al teléfono XXXXXXXXX.

Entiendo que una copia de esta ficha de consentimiento me será entregada, y que puedo pedir información sobre los resultados de este estudio cuando éste haya concluido. Para esto, puedo contactar a al responsable de la investigación al teléfono anteriormente mencionado.

Nombre del Participante (En letras de imprenta) | Firma del Participante | Fecha

ANEXO 2: CARTA DE CONFIDENCIALIDAD

CARTA DE CONFIDENCIALIDAD

Lima, DIA de MES de 2015

Señor
NOMBRES Y APELLIDOS DEL ENTREVISTADO
Entidad Pública
Dirección
Distrito.-

Tengo el agrado de dirigirme a usted, a fin de informarle que actualmente me encuentro realizando una investigación denominada:

"Factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en las Entidades de la Administración Pública según la NTP- ISO/IEC 27001" para optar por el Titulo de Magister en Gobierno de Tecnologías de la Información en la Universidad Nacional Mayor de San Marcos.

La investigación tiene como propósito realizar un estudio que recoja de manera organizada y estructurada las restricciones que encuentran las gerencias de Informática de las entidades del Sistema Nacional de Informática en el Perú para la implementación del Sistema de Gestión de Seguridad de la Información -SGSI- según la NTP-ISO/IEC 27001.

Considerando que la ONGEI ha determinado el uso obligatorio respecto de la implementación del Sistema de Gestión de Seguridad de la Información según la NTP-ISO/IEC 27001 en todas las entidades integrantes del Sistema Nacional de Informática y que ***NOMBRE ENTIDAD PUBLICA*** está definida como responsable de su implementación según cronograma incremental publicado, ha sido seleccionado dentro la muestra de investigación.

Para llevar adelante la investigación, es de vital importancia realizarle una entrevista en su calidad de *CARGO* de la *NOMBRE DE LA OFICINA/ÁREA/GERENCIA DE LA ENTIDAD* con la finalidad de obtener la información primaria que respalde la investigación, informo también que la entrevista será grabada y transcrita en texto para fines del análisis cualitativo de los datos.

Yo, como autor de la tesis, me comprometo formalmente a guardar total confidencialidad sobre la información obtenida a consecuencia de la entrevista, la misma que solo será utilizada para el sustento y actividades necesarias dentro de la investigación.

Por lo expuesto solicito su valiosa colaboración y la firma del formato adjunto referido al Consentimiento Informado para cumplir con los estándares de investigación.

Sin otro particular, quedo de usted,

Atentamente,

_____

Javier Alfonso Seclén Arana
DNI N°

ANEXO 3: PROTOCOLO DE PREGUNTAS PARA LA ENTREVISTA

1. **Identificación**
    a. Se comunica al entrevistado el momento que se inicia la grabación.
    b. El entrevistador se presenta, indica la fecha y hora y revisa el formato del compromiso informado.
    c. Preguntar al entrevistado su nombre completo, su cargo, el tiempo que lleva en el cargo y el tiempo en la institución.
2. **Contexto:**
    a. El entrevistador explica el propósito del estudio, y una pequeña explicación del proyecto de investigación.
3. **Entrevista:**

Fecha: _____ **Hora:** _____

Lugar (ciudad y ubicación específica): _____

Entrevistador: _____

Entrevistado (nombre, edad, género, puesto, gerencia o departamento):

_____

GUÍA DE PREGUNTAS:

I - Dimensión Técnica	(Preguntas referidas con la experiencia laboral/personal en Seguridad de Información)
1	¿Cómo define Ud. lo que es Sistema de Gestión de Seguridad de la Información?
2	Mencione su experiencia profesional (o personal) respecto de la Seguridad de la Información
3	¿Pertenece Ud. (o ha pertenecido) a alguna asociación vinculada a la Seguridad de la Información?

II - Dimensión del Proyecto	(Preguntas referidas a la Norma Técnica -NTP 27001- de Seguridad de Información)
1	¿Qué es la NTP-ISO/IEC 27001 y qué papel cumple la ONGEI en la implementación de esta norma?
2	¿Qué objetivos busca el Estado Peruano con la implementación de esta norma (NTP-ISO/IEC 27001) en la Administración Pública?
3	¿Qué factores cree Ud. que impactan o influyen en la implementación de la NTP-ISO/IEC 27001 en el Estado Peruano?

4	¿Tiene Ud. conocimiento de NTP de Seguridad de la Información anteriores a la actual (27001)?
5	¿Tiene Ud. conocimiento de algún caso de éxito de alguna Empresa (Pública o Privada) que haya implementado la NTP 27001 o anteriores?
6	Hace poco se ha aprobado la NTP 27001:2014, ¿Ud. cree que esto beneficiará más o no la implementación de la NTP 27001 en el Estado?

III - Dimensión Institucional	(Preguntas referidas a la Seguridad de la Información en su Institución)
1	¿Cómo cree Ud. que ayudaría (o viene logrando) en su Institución la implementación de la NTP-ISO/IEC 27001? (Beneficios que se lograrían con ello)
2	En su Institución, ¿Existe el apoyo de la Alta Dirección para la implementación de la NTP-ISO/IEC 27001? (SGSI)
3	¿En qué nivel/fase de la implementación incremental de la NTP 27001 se encuentra su institución?
4	Existe un presupuesto asignado de forma exclusiva para la implementación del SGSI (en su Institución)?
5	¿Cree Ud. que la Alta Dirección (de su Institución) tiene claro que es el SGSI y la importancia de implementarlo? Si es afirmativo ¿Por qué lo cree así?
6	Según su parecer ¿la Alta Dirección le ha brindado el respaldo necesario para el desarrollo de este Proyecto?
7	¿Está de acuerdo con que el Área de TI/Informática/Sistemas sea la encargada de llevar a cabo la implementación del SGSI? Si no es así, ¿Qué área sería la encargada de realizarlo?
8	¿Tiene definido un Comité Técnico y/o un Comité de Gestión de Seguridad de la Información en su institución?
9	¿Recibe (o ha recibido) capacitación sobre seguridad de la información en la dependencia donde Ud. trabaja? Si ha recibido, ¿Es permanente o esporádicamente?
10	¿Tiene definido el Alcance del SGSI para la implementación de la NTP 27001?
11	El Alcance del SGSI que se ha determinado, ¿está basado en algún proceso de negocio institucional?
12	A su parecer, ¿La estructura organizacional actual favorece o restringe el desarrollo del proyecto del SGSI en su Institución?
13	Tiene Ud. la metodología de Gestión de Riesgos que aplicará en la implementación del SGSI en su Institución? ¿Cómo determinó dicha metodología?
14	¿Cómo percibe Ud. la cultura organizacional en su Institución respecto del cumplimiento de la Seguridad de la Información en su Institución?
15	¿Existe en su entidad algún plan oficial de concienciación al personal de la Seguridad de la Información?
16	¿Qué otros factores cree Ud. que impactan o impiden la implementación de la NTP-ISO/IEC 27001 en la Administración Pública?

4. Cierre:
    a. El entrevistador agradece al entrevistado por su colaboración.
    b. Se comunica al entrevistado el momento que termina la grabación.

ANEXO 4: RECOMENDACIONES A TENER EN CUENTA EN LA ENTREVISTA

1. El propósito de las entrevistas es obtener respuestas sobre el tema de investigación en los términos, el lenguaje y la perspectiva del entrevistado. (es decir, “en sus propias palabras”)

2. Es esencial lograr neutralidad, espontaneidad y amplitud de respuestas durante la entrevista.

3. Es muy importante que el entrevistador genere un clima de confianza con el entrevistado y desarrolle empatía con él.

4. Es indispensable no preguntar de manera tendenciosa o induciendo a la respuesta.

5. No se deben utilizar calificativos.

6. Se debe escuchar activamente, pedir ejemplos y hacer una sola pregunta a la vez.

7. Debe buscarse identificación con el entrevistado, compartir conocimientos y experiencias y responder dudas pero manteniendo su papel como investigador. (Respecto a si el entrevistador debe hacerse amigo del entrevistado)

8. Debemos evitar elementos que obstruyan la conversación.

9. Es recomendable no saltarse “abruptamente” de un tema a otro, sino profundizar en el asunto.

10. Siempre resulta conveniente informar al entrevistado sobre el propósito de la entrevista y el uso que se le dará a ésta.

11. La entrevista debe ser un diálogo y resulta importante dejar que fluya el punto de vista único y profundo del entrevistado.

12. Normalmente se presentan primero las preguntas generales y luego las específicas.

13. El entrevistador tiene que demostrar interés en las reacciones del entrevistado al proceso y a las preguntas.

14. Cuando el entrevistado no le quede clara una pregunta, es recomendable repetirla.

15. El entrevistador debe estar preparado para lidiar con emociones y exabruptos.

16. Cada entrevista es única y crucial, y su duración debe mantener un equilibrio

ANEXO 5: ESQUEMA DE PLANEACIÓN DE LA ENTREVISTA CUALITATIVA

Al inicio de la entrevista

1. Apague su teléfono celular
2. Platicar sobre un tema de interés y repetir el propósito de la entrevista, la confidencialidad de la misma, el consentimiento informado, etc.
3. Solicitar permiso del entrevistado para grabar y tomar notas.
4. Comenzar la entrevista.

Durante la entrevista

1. Escuchar activamente, mantenga la conversación y no transmita tensión.
2. Sea paciente, respete silencios, tenga un interés genuino.
3. Asegurarse de que el entrevistado terminó de contestar una pregunta antes de pasar a la siguiente.
4. Dejar que fluya la conversación.
5. Tomar notas y grabar la entrevista (estas grabaciones deben ser lo más discretas posibles)
6. Demostrar aprecio por cada respuesta.

Al final de la entrevista

1. Preguntar al entrevistado si tiene algo que agregar o si tiene alguna duda.
2. Agradecer por el tiempo invertido y explicar nuevamente lo que se va a hacer con los datos recolectados en dicha entrevista.

Después de la entrevista

1. Hacer un resumen de la entrevista.
2. Colocar a quien se entrevistó en su contexto (¿qué me dijo?, ¿por qué me lo dijo? ¿cómo transcurrió la entrevista?)
3. Revisar las anotaciones de campo.
4. Transcribir la entrevista lo más rápido posible.
5. Enviar una carta de agradecimiento o un e-mail.
6. Revisar el protocolo de preguntas de la entrevista y mejorarlo, si así lo considera necesario.

ANEXO 6: AYUDA MEMORIA PARA EL ENTREVISTADO

AYUDA MEMORIA PARA ENTREVISTADO DE TÉSIS

1°) Propuesta de Investigación

La presente investigación tiene como propósito realizar un estudio cualitativo que recoja de manera organizada y estructurada, a través de entrevistas, las restricciones que encuentran las gerencias de informática de las entidades del Sistema Nacional de Informática en el Perú para la implementación del Sistema de Gestión de Seguridad de la Información según la NTP-ISO/IEC 27001.

El Trabajo de Investigación es para acceder a la Maestría de Gobierno de TI en la Universidad San Marcos y tiene que ver con lo siguiente:

¿Qué factores afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades de la Administración Pública Peruana de acuerdo a la NTP- ISO/IEC 27001?

Las conclusiones que la investigación pretende obtener podrían ser utilizadas como información que nos permita llegar a una comparación objetiva respecto de los logros y avances obtenidos en Seguridad de la Información y evaluar los factores que no permiten el desarrollo continuo y progresivo del proceso de implementación del Sistema de Gestión de Seguridad de la Información en la Administración Pública Peruana.

2°) Unidad de Análisis

La unidad de análisis para la presente investigación está compuesta por los gerentes de Informática u oficiales de seguridad de la información de las entidades responsables de la implementación del Sistema de Gestión de Seguridad de la Información que son de cumplimiento obligatorio según la NTP-ISO/IEC 27001.

3°) Población

Para el proyecto de investigación, se ha identificado que el universo de informantes está conformado por las gerencias de informática u Oficiales de Seguridad de Información de las entidades públicas responsables de llevar a cabo la implementación de la NTP-ISO/IEC 27001.

4°) Entrevistas a realizar

Para el trabajo de investigación es necesario desarrollar entrevistas especializadas a las Instituciones del Estado que estén obligadas a su implementación (según especificación de la NTP-ISO/IEC 27001). Por ello, y en base a las coordinaciones realizadas, recurro a sus buenos oficios que me permitan llegar a la conclusión de la tesis de la maestría descrita.

Con este fin, le adjunto el Protocolo de Preguntas que se realizaría en dicha entrevista respecto del problema de investigación propuesto. Estas preguntas no tienen que ser resueltas en su totalidad si no es necesario, y además, podrían incorporarse otras adicionales si durante la entrevista fuera necesario.

ANEXO 7: NTP-ISO/IEC 27001:2014 (R.M. N° 004-2016-PCM)

ANEXO 2

RELACIÓN DE REPRESENTANTES DEL GOBIERNO NACIONAL ANTE COMISIÓN INTERGUBERNAMENTAL DEL SECTOR AGRICULTURA Y RIEGO, CONFORMADA EN EL MARCO DEL DECRETO SUPREMO Nº 047-2009-PCM

	CARGO	DEPENDENCIA / INSTITUCIÓN	CARGO
1	Viceministro (a) de Política Agrarias	Despacho Viceministerial	Presidente Comisión Intergubernamental
2	Director (a) de la Oficina General de Planeamiento	Oficina General de Planeamiento y Presupuesto	Miembro
3	Profesional		Miembro Alterno
4	Profesional	Oficina General de Asesoría Jurídica	Miembro
5	Profesional	Oficina General de Administración	Miembro
6	Profesional	Oficina General de Gestión de Recursos Humanos	Miembro
7	Director (a) General de Articulación Intergubernamental	Dirección General de Articulación Intergubernamental	Miembro
8	Director (a) de Gestión Descentralizada		Miembro
9	Director de Seguimiento y Evaluación de Políticas (a)	Dirección General de Seguimiento y Evaluación de Políticas	Miembro
10	Director (a) de Estadística Agraria		Miembro Alterno
11	Director (a) General de Políticas Agrarias	Dirección General de Políticas Agrarias	Miembro
12	Director (a) de Políticas y Normatividad Agraria		Miembro
13	Profesional	Dirección General de Negocios Agrarios	Miembro
14	Profesional		Miembro Alterno
15	Profesional	Dirección General de Asuntos Ambientales Agrarios	Miembro
16	Profesional	Dirección General de Infraestructura Agraria y Riego	Miembro
17	Profesional	Servicio Nacional Forestal y de Fauna Silvestre	Miembro
18	Profesional		Miembro
19	Profesional	Programa de Desarrollo Productivo Agrario Rural - AGRORURAL	Miembro
20	Profesional		Miembro Alterno
21	Jefe (a) del Programa	Programa de Compensaciones para la Competitividad - AGROIDEAS	Miembro
22	Jefe (a) de la Unidad de Planificación, Seguimiento y Evaluación		Miembro
23	Director (a) de Gestión del Riego	Programa Sub Sectorial de Irrigaciones (PSI)	Miembro
24	Profesional		Miembro Alterno
25	Director (a) de la Unidad de Estudios y Cooperación de la Oficina de Planificación y Desarrollo Institucional	Servicio Nacional de Sanidad Agraria (SENASA)	Miembro
26	Profesional		Miembro
27	Director (a) General de la Oficina de Planeamiento y Presupuesto	Instituto Nacional de Innovación Agraria (INIA)	Miembro
28	Profesional		Miembro Alterno
29	Director (a) de Conservación y Planeamiento de Recursos Hídricos	Autoridad Nacional del Agua (ANA)	Miembro

1332846-1

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL
Nº 004-2016-PCM

Lima, 8 de enero de 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008;

Que, la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", aprobada mediante Resolución Nº 42-2008/INDECOPI-CNB, por la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.2ª Edición" aprobada por Resolución Nº 129-2014/DNB-INDECOPI;

Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo Nº 063-2007-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), siendo ésta la encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo Nº 066-2011-PCM, establece en su Objetivo Nº 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia Nº 4, la implementación de mecanismos para mejorar la seguridad de la información, la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo Nº 081-2013-PCM, prevé determinados Lineamientos Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema

Nacional de Informática, para el caso ONGEI-PCM, a cargo de implementar dicha Política Nacional, articular la implementación efectiva del acotado lineamiento por parte de los distintos entes del sector público;

Que, estando a lo indicado en los considerandos precedentes la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros a través del Memorando Nº 152-2015-PCM/ONGEI, recomienda la aplicación y uso de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo;

De conformidad con lo dispuesto en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado; y, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo Nº 063-2007-PCM y sus modificatorias;

SE RESUELVE:

Artículo 1.- De la aprobación

Apruébese el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Artículo 2.- Publicación

La Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" será publicada en el Portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y en el Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) (www.ongei.gob.pe) el mismo día de la publicación de la presente resolución en el Diario Oficial El Peruano.

Artículo 3.- De la implementación

Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma.

Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

La ONGEI brindará asistencia técnica a las entidades que lo requieran. Las entidades públicas que a la fecha cuenten con la certificación ISO 27001, están exoneradas del presente proceso de implementación.

Artículo 4.- De la certificación de la norma

Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2 Edición"; podrán realizar dicha certificación de forma opcional y con recursos propios de cada entidad.

Artículo 5.- Del Comité de Gestión de Seguridad de la Información

Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por:

- El/la titular de la entidad;
- El/la responsable de administración o quien haga sus veces;
- El/la responsable de planificación o quien haga sus veces;
- El/la responsable del área de informática o quien haga sus veces;
- El/la responsable de área legal o quien haga sus veces y
- El/la oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad de acuerdo a la norma que se aprueba mediante el Artículo 1º de la presente Resolución Ministerial.

Artículo 6.- De la responsabilidad de la implementación

La responsabilidad de la implementación de la presente norma será del titular de cada entidad.

Artículo 7.- Déjese sin efecto

Deróguese la Resolución Ministerial Nº 129-2012-PCM.

Regístrese, comuníquese y publíquese.

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

1333015-1

AGRICULTURA Y RIEGO

Delegan facultades a diversos funcionarios del Ministerio durante el Ejercicio 2016

RESOLUCIÓN MINISTERIAL
Nº 0006-2016-MINAGRI

Lima, 12 de enero de 2016

CONSIDERANDO:

Que, mediante la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, se definen las funciones generales y la estructura orgánica de los Ministerios, precisando en el último párrafo de su artículo 25, que los Ministros de Estado pueden delegar, en los funcionarios de su cartera ministerial, las facultades y atribuciones que no sean privativas a su función, siempre que la normatividad lo autorice;

Que, de acuerdo a lo dispuesto en el último párrafo del artículo 9 del Decreto Legislativo N° 997, Decreto Legislativo que aprueba la Ley de Organización y Funciones del Ministerio de Agricultura, modificado por la Ley N° 30048, en adelante la LOF del MINAGRI, el Ministro puede delegar las facultades y atribuciones que no sean privativas a su función;

Que, el tercer párrafo del literal c) del artículo 8 de la Ley N° 30225, Ley de Contrataciones del Estado, señala que el Titular de la Entidad podrá delegar, mediante resolución, la autoridad que dicha Ley le otorga, salvo los casos expresamente previstos en el referido literal;

Que, según el numeral 7.1 del artículo 7 del Texto Único Ordenado de la Ley Nº 28411, Ley General del Sistema Nacional de Presupuesto, aprobado mediante Decreto Supremo Nº 304-2012-EF, el Titular de una Entidad es la más alta Autoridad Ejecutiva y puede delegar sus funciones en materia presupuestal cuando lo establezca expresamente, entre otras, la citada Ley General;

Que, asimismo, el numeral 40.2 del artículo 40 del referido Texto Único Ordenado de la Ley Nº 28411, establece que las modificaciones presupuestarias en el nivel Funcional Programático son aprobadas mediante Resolución del Titular, a propuesta de la Oficina de Presupuesto o de la que haga sus veces en la Entidad, y que el Titular puede delegar dicha facultad de aprobación, a través de disposición expresa, la misma que debe ser publicada en el Diario Oficial El Peruano;

ANEXO 8: TRANSCRIPCION DE LA 1ra. ENTREVISTA

Mi primera consulta es dentro de la **Dimensión Técnica**, y es:

Yo: ¿Cómo define Ud. lo que es un Sistema de Gestión de Seguridad de Información?
E: Un sistema de seguridad de información básicamente es el conjunto de procesos para gestionar eficientemente el acceso a la información buscando la confidencialidad, integridad y disponibilidad y eso, a su vez, es para reducir riesgos de seguridad de la misma información. Básicamente es eso.

Yo: Mencione su experiencia profesional respecto a la seguridad de información que ha venido teniendo en estos años
E: Yo he comenzado en la Administración Pública en el año 1998 en el cual he sido Administrador de Red en el Ministerio de Agricultura; durante todos esos años me he desempeñado en la parte de administración de redes viendo implementaciones de correo, servicios de comunicaciones, servicios de firewall, en algunos momentos hasta instalaciones de BD, temas de redes, equipos de comunicación y, a través de los años he estado trabajando en el año 2004, en (el Ministerio de) Migraciones que también me he desempeñado en temas de redes y comunicaciones. Ya para el año 2008 ingresé a la Agencia de Promoción de Inversiones - PROINVERSION -que pertenece al MEF- en el cual ingresé como Especialista en Seguridad de Información, en pocas palabras los comienzos de lo que era el Oficial de Seguridad que estaba dentro de la Oficina de Sistemas y en el cual había ya comenzado la creación de un Comité interno para hacer frente de algún problema de seguridad de información de la institución y tomar decisiones en conjunto
Yo: ¿Qué era como un PECERT entonces (interna)?
E: Era básicamente el PECERT es una entidad que reúne a gente de seguridad para un tema determinado para afrontar un problema. No, en este caso son de diferentes áreas en el cual se tenía que tomar la decisión, previamente información del incidente para que ellos en conjunto puedan elaborar una respuesta a tal incidente. Pero que no llegaba a la Alta Dirección. O sea, solamente llegaba a nivel operativo.

Yo: Continuamos con la Dimensión del Proyecto
Es decir, preguntas referidas al proyecto mismo, a la misma Norma Técnica Peruana 27001 de Seguridad de la Información. Es la parte más dimensionada al sistema, a la propia norma se puede decir.

Yo: ¿Podría referirme Ud. de qué trata esta NTP 27001 y que papel cumple la ONGEI en la implementación de esta norma?
E: La (NTP) 27001 es básicamente la implementación de un Sistema de Gestión de Seguridad de la Información. Ese sistema, como te había respondido en la primera pregunta, se refiere a implementar los mecanismos para asegurar y proteger la información. El tema viene en que esta norma -la 27001- es una norma internacional en el cual se ha tomado como referencia el año 2005, es una norma del 2005 internacional en el cual ha sido actualizada por el Estado Peruano en el año 2008. Ahora, ya ha sido aprobada la 27001:2013 y, tengo entendido, que el próximo año, debe estar saliendo -emitida por INDECOPI- la 27001:2014 para el Estado Peruano.

Yo: ¿Y qué papel cumple la ONGEI en esta implementación?

E: La ONGEI es el ente normativo de informática a nivel del Estado Peruano, es un organismo que depende de la Presidencia del Consejo de Ministros. No es una entidad netamente autónoma, tiene ciertas limitaciones pero es una parte importante para dirigir a las demás entidades del Estado -en temas informáticos- del Sistema Nacional de Informática. Es el que regula, norma, nos orienta a utilizar estas normas y a unas buenas prácticas para todo lo referente a lo que son sistemas de información, seguridad de información, etc.

Con sus dificultades del caso, como cambios casi seguidos que hace que su labor de apoyo se vea disminuida y cada vez que empieza a retomar fuerza, ocurren estos cambios, el cual perjudica y atrasa quizás los proyectos que se tengan pensados a nivel del Estado.

Yo: ¿Cómo esta norma?
E: Si.

Yo: ¿Qué objetivos cree Ud. que busca el Estado Peruano con la implementación de esta norma en la administración pública? ¿Qué objetivos se persiguen? ¿Cuál es la finalidad de esta norma?
E: Básicamente en implementar mecanismos de seguridad para la información. Ese es netamente el objetivo principal y el otro objetivo sería la metodología más eficaz para poder implementar de mejor manera la seguridad de la información. En esos dos puntos principales es el objetivo del Estado para este tipo de norma.

Yo: ¿Tiene conocimiento de normas técnicas de seguridad anteriores a la actual norma?
¿Sabe si ha habido normas anteriores a ésta?
E: Si, casualmente el Estado tal como le he manifestado, yo vengo siguiendo de cerca cómo ha ido evolucionando la ONGEI como tal y, en su oportunidad el Estado Peruano creó o mejor dicho aprobó la NTP 17799 que es un conjunto de buenas prácticas para asegurar los sistemas de información conjuntamente con la 12207 de ciclo de software. Conjuntamente sacó esas dos normas me parece que en el año 2009 o 2010. Y, mediante cronogramas, solicitaba de que actualice y que implementen esas buenas prácticas en las entidades informáticas del Estado. Y eso fue una tarea complicada porque las entidades no tenían conocimiento exacto de cómo implementarlas, cogían esa norma como sustento para los pedidos de compras o en forma aisladas. Por ejemplo, yo necesito seguridad para un firewall, bueno jalaba un dato de ahí para sustentar. Necesitaba poner seguridad en el Data Center, ¿A ver qué cosa hay por acá? jalaba lo que necesitaba

Yo: ¿O sea que aprovechaban para el presupuesto?
E: Si. Y es válido, pero no se tenía el conjunto de las acciones informáticas y de sistemas de información que se puedan monitorear y avanzar. Todo era aislado. Permisos, contraseñas...ah, acá hay contraseñas, pero no estaban interrelacionadas las cosas. Entonces, ese era el gran problema de esa norma, de la (NTP) 17799. Por tal razón es que la ONGEI convocaba a reuniones a fin de ver un mecanismo de que esa norma sea implementada de la mejor manera en el Estado. Tal es así que, cogieron la (NTP) 27001, en el cual te aterrizaba de qué manera es que tú podías implementar eficazmente la (NTP) 17799, que actualmente es la 27002.

Entonces, al implementar la 27001, aterrizaba el tema en sí de cómo comenzar y a qué implementar el tema de las buenas prácticas de la (NTP) 17799. Entonces, te decía: Ahí tienes, dentro de tus procesos, el Alcance y ahí enfocabas y ahí tenías todas las buenas prácticas para implementar la seguridad con la que tú ya habías determinado ese Alcance. Ahí aterrizabas

Yo: Pero como toda norma ISO, una norma ISO te dice que debes hacer, no el cómo
E: Bueno, la norma ISO o la de calidad te dan pautas para que tu cojas lo necesario, lo que necesitas.

Osea, te dicen, estos 10 pasos te recomiendo. Perfecto, pero en mi realidad yo cojo 5 de estas, y esas 5 sí tengo que cumplirlas. No necesito las 10. La norma se adecúa a mi idiosincrasia, a mi necesidad.

Yo: ¿Sabe si alguna de estas normas anteriores a la 27001, han sido implementadas con éxito acá en el Perú?
E: Yo tengo entendido que las entidades como INDECOPI y la ONP, que actualmente tienen la (NTP) 27001 para un determinado proceso ya lo tenían implementado pero sin que esté enfocado en un sistema de seguridad de información. Implementaron los dominios de que consta la (NTP) 17799 y haciendo un análisis de brecha, con lo que tenían ellos más con la norma, haciendo un análisis gap podían determinar qué cosa era lo que les faltaba y han ido paulatinamente corrigiendo y han mantenido los controles con los dominios de la (NTP) 17799. Pero, no aterrizaron a un sistema, a un proceso en si como es la (NTP) 27001.

Yo: ¿Se podría decir que anteriormente aún no ha sido implementado con éxito?
E: Si, pero la 17799 como tal, se ha implementado pero a nivel no netamente de un proceso sino global. O sea, tengo mis brechas.

Yo: Cuando dice a nivel global, ¿Se refiere a toda la institución o solo al área de Informática?
E: Efectivamente, estaba más enfocada a temas de seguridad de sistemas de información, sistemas de comunicaciones, etc. No iba más allá. Si bien es cierto esa norma (NTP 17799) es tan importante, por esa razón es que ha sido incluida como un anexo a la (NTP) 27001. Por eso podemos ver en la 27001 como implementar el sistema de gestión de seguridad de información, etc. y el comienzo de cómo llegar al Alcance es por intermedio de la 27003 y cogiendo la 27005 que es de riesgos ya vas determinando el tema de tu sistema de gestión de seguridad de información, pero todo eso está en base a los controles que tienes con la 27002 que es la 17799. Por eso es que está como anexo, tú puedes ver en la norma, al final. La misma norma 17799 menos detallada está en la 27001

Yo: Entonces, actualmente, con la 27001 ¿Ya se han implementado con éxito?
Quería adicionar algo más, con el tema de la 17799 también utilizaban COBIT y también utilizaban como referencia los exámenes de control de Contraloría. Entonces, toda esa información les servía como para poder corregir e ir puliendo todos los temas de seguridad, de la parte informática. Se utilizaba una serie de buenas prácticas, ITIL también por ejemplo. Y todo en conjunto hacía que puedas

sobrellevar el tema de la implementación de la seguridad. Con eso sobrellevabas, pero ¿Qué dice el sistema de gestión de seguridad de información? Que tienes que tener unos controles, que eso tiene que estar enmarcado en un previo Alcance, en un Análisis de Riesgos; y de acuerdo a ese análisis de riesgos, implementar tus controles. Yo eso tiene que ser retroalimentado para que posiblemente pueda ser revisado por el área de auditoria de la institución y posteriormente pueda ser certificado. ¿Y qué se necesita para eso? de que sea un proceso core del negocio y a su vez que no sea muy ambicioso, que sea lo más preciso; para que posteriormente, de ese subproceso de que se haga el sistema de seguridad de información, pueda ser replicado en otro proceso y a su vez se pueda ir ramificando y sensibilizando a las demás áreas para que vayan implementando el tema de seguridad de información en sus áreas

Yo: ¿Sabe si han habido casos de éxito de esta implementación en empresas privadas?
E: Lo que hay que recalcar es lo siguiente: El SGSI reposa en un proceso core del negocio, en el cual lo ideal sería que sea un subproceso para que pueda llegar e implementar todos los pasos para poder tener esos controles.
Ahora, la realidad del Estado Peruano es la siguiente: Normalmente, se dice que las áreas estratégicas y funcionales deben ser las que más o menos se deban tener como proceso pero no se toman los órganos de apoyo. Y, como el problema viene que, en las áreas funcionales y estratégicas, no están muy metidas en este tema. El tema viene de que tienen que ser una extrema comunicación, reuniones, etc. para poder sacar la información necesaria y, a su vez, viendo qué punto es el cual todos los procesos convergen o tienen algo que ver. Entonces, lo que se está optando acá es utilizar un órgano de apoyo como parte de los procesos del SGSI. Y, en este caso, se está tomando o los centros de datos o los sistemas de información.

Yo: ¿Cómo órganos de apoyo, como centros de apoyo?
E: Claro, los órganos de apoyo son la parte de administración, OGPP, o sea los de apoyo. No son las áreas estratégicas: Dirección General de Estrategias para las Comunicaciones, Dirección General de Consulados. Por ejemplo, nuestra área está en la Dirección General de Comunicaciones y dentro de ahí está la oficina de TI y otras dos entidades más, dos oficinas más. ¿Te das cuenta?

Yo: ¿O sea que no llegan a ser un órgano de línea directa?
E: No. Y a su vez, estamos a la par de OGPP. Pero, sin embargo, todos los sistemas de información reposan en nuestro centro de datos que lo administra la Oficina de TI. Por lo tanto, muchas de las Entidades, y particularmente mi persona, hemos determinado que este centro de datos sea nuestro alcance, pudiéndose aún reducirse. Podría ser: Gestión de la infraestructura del centro de datos, Gestión de los sistemas de información almacenados en el centro de datos. Eso es lo que ha hecho la ONP, la ONPE e INDECOPI. Aunque, en éste último hay que ser honestos en decir que ellos han implementado más procesos. Ellos están más adelantados que todos. Incluso la ONP creo que tiene su SGSI en su Servicio de Atención al Cliente. Eso sí habría que validarlo. Pero en resumen, son pequeños procesos en el cual la entidad tiene su 27001.

Yo: Pero en el caso de la ONP, acaso su objetivo no es una mejor atención a sus clientes? Tal vez hayan visto allí su proceso core
E: Bueno, Gestión del Cliente va afín, pero previamente hizo de su centro de procesamiento de datos. En todo caso, la primera implementación del SGSI sirve como base para las demás.

Yo: Entonces, ¿Es importante que la primera (implementación del SGSI) no sea tan amplia?
E: Claro, no puede ser muy ambiciosa. Y segundo, hay un tema de replicación para las demás. A su vez, ¿Por qué se determina el Alcance dentro de la oficina de TI? No porque deba ser, sino porque todas las personas involucradas y los actores, trabajan contigo. Entonces, tienes la oportunidad de conversar y preguntar con el de Base de Datos, con el de Desarrollo, con el de Redes, con el de Infraestructura; les haces sus cuestionarios, conversas, lluvia de ideas, etc. armas tu análisis de riesgo. Entonces, directamente puedes hacer el trabajo. A diferencia de un proceso adicional, de otro proceso que no esté dentro. Conversar con un proceso que vaya a 03 áreas, así sea chiquito, tienes que conversar con la gente de una de las áreas, con la gente de la otra área, y a veces no tienen la disponibilidad ni las ganas.

Yo: Respecto a la <u>Dimensión Institucional</u>, referido a la Seguridad de la Información en su institución, ¿Cómo cree Ud. que ayudaría que se implemente en su institución la NTP 27001? ¿Cuáles serían los beneficios que se lograrían? ¿Para qué ayudaría esta implementación?
E: Primero, para tener controles definidos para poder reducir problemas de seguridad de información que sean medibles, cuantificables y que me permitan poder replicar todos estos controles a nivel institucional (en el tema de seguridad de información). Básicamente esa es la finalidad de implementar.

Yo: ¿Cree que le daría más imagen a la institución también?
E: Por supuesto que sí. Hay un tema de imagen, el cual se ven replicados los servicios que brindamos y en el cual se ve reflejado no solamente la calidad de los mismos sino lo seguro que podemos ser y a la vez brindar a la ciudadanía en general, teniendo en cuenta que en nuestro caso, ésta no es sólo local sino también a nivel internacional por el tema de las misiones que comprenden los consulados, las embajadas, etc. Eso es más ambicioso.

Yo: Eso sería el mayor beneficio, ¿Es así?
E: Claro. Que sea medible, cuantificable y que a su vez nos proporcione la mejor manera de tener un control de toda la seguridad y a su vez el tema de imagen institucional, no solamente nacional sino también internacional.

Yo: Respecto de la implementación de la NTP 27001 ¿Existe apoyo de la Alta Dirección en su institución?
E: Bueno, haciendo una retrospectiva en otras entidades, hay de todo. Hay indiferencia, hay poco interés, hay mucho interés, etc. Puedo decirte por ejemplo que en el Ministerio de Trabajo hay plena disposición. En esta actual, se puede decir que no hay el suficiente apoyo debido a un tema más de sensibilización por la Alta Dirección. Es decir, hacerle llegar a ver las consecuencias de no implementar un sistema de gestión de seguridad de la información

Yo: Entonces ¿No lo tienen bien claro?
E: Simplemente no lo entienden. No han percibido algún problema hasta el momento.

Yo: O sea que tal vez cuando tengan un problema de seguridad de información es realmente cuando se darán cuenta
E: Las implementaciones de seguridad que se están ya implementadas, están dando la seguridad momentánea. Pero eso no significa que podamos estar sujetos a otro tipo de ataques y a accesos no autorizados de información o a "Defacements" que puedan perjudicar nuestra imagen institucional. Entonces, te puedo decir que la situación actualmente no hay el apoyo necesario y justamente mi tarea se centra en lograr que ellos se sientan identificados, entiendan y den ese apoyo necesario. Ya que como te había manifestado, hay instituciones que han implementado comités internos, por que la decisión -al ser internas- son comités técnicos pero, que la institución al no tener bien claro esto, son el comité de seguridad de información que toma decisiones internas pero no a nivel institucional o de Alta Dirección. Por eso, el proceso debería ser el siguiente:

1° Oficializas quien va a hacer las labores de Oficial de Seguridad de Información a la ONGEI.

2° Conformas el Comité Ejecutivo de Seguridad de Información, en el cual está la Alta Dirección. Este es el comité de Gestión, el cual toma decisiones.

3° A su vez, conformas con un menor rango, un comité operativo, el cual se dedica a hacer la parte técnica para que, en coordinaciones con el Oficial de Seguridad, presenta a la Alta Dirección la documentación para su aprobación o no aprobación.

Así trabajas. Pero si nosotros tenemos un comité interno operativo y presentamos un documento a la Alta Dirección, ellos van a decir: ¿Qué es esto? No lo entiendo. Pero si a la Alta Dirección o al Titular se le envía un documento que está firmado por el Secretario General, por las Direcciones de Línea o por el Viceministro, ahí si lo consideran.

Yo: ¿Es importante tener el Comité de Gestión entonces?
E: Por supuesto. El Comité de gestión de Seguridad de Información es imprescindible para que haya un Sistema de Gestión de Seguridad de Información.

Yo: ¿En qué nivel o fase de la implementación incremental de la NTP 27001 se encuentra su institución?
E: Estamos en la fase inicial. Estamos en el tema de la conformación de los comités, la determinación del Alcance, Organizar los activos para posteriormente elaborar el análisis de riesgo, el tema de aplicabilidad, o sea estamos en esa etapa inicial, no se ha avanzado más. El objetivo mío es, por lo menos este año, culminar la fase I.

Yo: ¿Existe un presupuesto asignado de forma exclusiva para la implementación de la seguridad de la información en su institución?
E: Sí y no. Es decir, en mi institución tenían un concepto de que para implementar un SGSI como tal, se requería de un personal para personal y para infraestructura.

Eso ha sido motivo de una reunión para aterrizarlo. Me acuerdo que en la entrevista de trabajo me preguntaron por una herramienta que se llama PULPO.

Yo, particularmente, fui sincero y les dije que la verdad no lo recordaba. Entonces el que me preguntó dijo "No es importante", "quería saber nomás". Pasada esa anécdota, conversando con el personal de desarrollo me dice: "¿sabe qué? nosotros creemos de que para implementar el SGSI primero tenemos que tener el inventario de todo, segundo la infraestructura y tercero tener el personal"

Yo: ¿A qué se refiere con la infraestructura?
E: Ahí está. Implementar un sistema de gestión, como el que nos enseñó Frayssinet (ONGEI) en ese programa la vez pasada que hubo reunión de PCM. Pero, al igual del PULPO, necesito un hardware, necesito un software, necesito licencias, etc. Todo eso necesita, y de ahí el personal para que pueda administrar eso y pueda trabajar el inventario, etc. Y de ese personal, de repente tercerizar lo que falta. Entonces, la parte de infraestructura y la parte de tercerizar no lo entendían bien.

Yo: Entonces, ¿es como que a nivel institucional también como que no se entiende bien lo que hay que hacer?
E: Claro. Ellos pensaban eso, que sin el software no se podía implementar el SGSI. Se puede comenzarlo sin el software, porque lo bueno de nosotros en cierta forma es que el Estado se las ingenia. No necesito un software en el cual ingreso la data.

Yo: ¿Es como que les han vendido esa idea? De que si no tienes el software entonces no puedes hacer el SGSI
E: Claro. Pero ahora, tienes el software ¿Y quién lo va a administrar? la gente. No, así no es. El personal es la que cuenta primero y después posteriormente construyes la herramienta. Entonces yo le dije: mira, lo primero es la gente, ya la tienes. Está una Srta. que es especialista en seguridad informática y me tienes a mí que soy Oficial de Seguridad. Entonces, con este personal se va a ir haciendo la gestión de los trabajos para ir implementando el tema de las fases de la implementación del SGSI. La parte de infraestructura es opcional, porque de repente en algún momento se va a manejar tal cantidad de información, pero eso es cuando tienes el SGSI implementado, entonces puedes canalizarlo por allí.
Me dijeron: Ah ya ok. Yo tenía ese concepto inicial que te dije. Entonces vamos a tener que cambiar el chip.

Yo: ¿Primero la herramienta y después el personal?
E: Si. En vista de que cómo no tenían bien claro qué comprar, entonces traemos a la gente que sabía para saber qué comprar, me dicen.
Un momentito les dije, no hay porqué comprar nada todavía. No me amarro con ninguno. Déjame levantar la información, déjame trabajarlo, tener fase1, fase2 y fase3; y de ahí ir replicando y de recién quiero ver que hacer para que mi data ya la baje y pueda trabajar como debe ser.

Yo: O sea que ¿Se podría decir que la Alta Dirección no tiene claro lo que es el SGSI?

E: No solamente la Alta Dirección, sino hasta la propia área de informática no tenía bien claro cómo es que se implementa. Pero bueno, yo también en algún momento -a ti también te debe haber pasado lo mismo- ¿Cómo implemento? ¿Cómo hago?

Yo no sé. Entonces, decía: bueno, está la 17799, pero, ¿Y de ahí qué hago? Bueno, sencillo, determino el Alcance, análisis de riesgo con los activos que intervienen en dicho alcance y ahí haces las matrices para poder determinar cuál es lo principal y de ahí mecanismos de control para monitorear todo lo que, de acuerdo a tu análisis, es importante. Ahora, ¿Cómo hacer el seguimiento y el monitoreo? Allí hay unas técnicas, pero es así. Eso es el ciclo PDCA. Pero ojo, para hacer todo esto, no es sencillo tampoco.

Yo: ¿Y no es solamente el software verdad?
E: No. El software es solamente un complemento para que tú puedas administrar mejor el avance, reportes, etc. Pero todo puede estar canalizado manualmente o con una herramienta de Excel.

Yo: Según su parecer, ¿La Alta Dirección ha brindado el respaldo necesario para que se desarrolle o se inicie y se continúe la implementación de esta norma?
E: La respuesta es que no. Pero no porque no quieran, sino porque no han sido concientizados de la mejor forma. No saben la magnitud del problema que se puede dar al no implementar en la institución un SGSI.

Yo: ¿Está de acuerdo con que el área de TI o de informática o de sistemas -según como se llame en su entidad- sea la encargada de la implementación del SGSI en su institución?
E: No, porque el SGSI debe ser transversal a la institución. No debe depender, en cierta forma, de un área que puede ser juez y parte. El error que se suele cometer es que se asocia a seguridad de información con informática. Si bien es cierto que seguridad de información ve la parte de información, ya sea digital o física de los documentos, debe estar en un área en el cual pueda fiscalizar, pueda recomendar y pueda monitorear las actividades que se realizan ya sea para la implementación del SGSI o para las acciones de seguridad de la información netamente técnicas. El área que se encargue de la implementación debe estar en un área muy cercana a la Alta Dirección para los temas de ejecución directa o lo más rápida posible. Entonces, esa área debe estar fuera del área de TI. Dentro de la implementación de controles, puedes encontrar ciertas deficiencias. Entonces tú envías un informe que se lo envías a tu jefe mismo, y él mismo jefe te dirá: "Ok, si entiendo. Hay que corregir eso, pero ponlo de tal manera de que se está haciendo, suavízalo o no lo pases". Es diferente que si el documento viniera directamente del Secretario General, porque el informe de la persona encargada de seguridad de información no puede salir directo. Eso quiere decir que si yo estoy fuera del área, se lo envío al jefe y el secretario general directamente lo solicita. Entonces ya no hay un filtro.

Yo: Entonces, no debería ser directamente el área de TI ¿verdad?
E: No. Debería ser el área de Seguridad de Información, el cual debe componerse del Oficial de Seguridad y de las demás áreas nivel de seguridad informática; y dependiente de la Alta Dirección o de un área de jerarquía en esa institución.

Yo: En la institución, ¿Se ha recibido o se recibe actualmente capacitación sobre seguridad de la información?
E: Tengo conocimiento que no. Además, si yo no lo doy menos todavía.

Yo: ¿Y se tiene pensado brindar capacitación en seguridad de la información?
E: Si, claro que se tiene planificado. Invitar a la ONGEI, hacerlo yo también, proveedores. Es parte del trabajo.

Yo: ¿Tienen actualmente definido el Alcance con el que se va a trabajar el SGSI?
E: Tenemos en mente seguir el procedimiento que se viene optando a nivel de las instituciones. O sea, ir de frente al core del negocio dentro de TI que involucra a casi todas las áreas de la institución: y que puede ser el centro de datos.

Yo: ¿Eso se consideraría como un proceso o como un servicio?
E: Es un proceso si lo consideras como "proceso de gestión del centro de procesamiento de datos"

Yo: ¿Y ese proceso ya está definido, tú como Oficial tienes que definirlo o sino quien lo define?
E: Lo importante es que se tiene que tener dominado el tema de procesos. Por ejemplo, si el proceso dentro la institución está definido en oficina de métodos de OGPP (Planificación y Presupuesto), tienes el proceso macro pero no tienes procesos específicos, entonces tienes que revisar e implementar un proceso, que si bien es cierto no está detallado y no está con su diagrama de flujo ni sus procedimientos, nosotros tenemos que determinarlo. Por ejemplo, el subproceso "soporte de infraestructura" es parte del proceso "gestión de TI".

Yo: Entonces, ¿Se podría decir que el encargado de implementar el SGSI en la institución, tiene que tener conocimientos de procesos?
E: Si, tiene que tener conocimientos de procesos. Es importante que tenga ese conocimiento para que pueda ver como un proceso se interrelaciona con los demás. No se necesita tampoco un erudito para determinar que el centro de datos no se interrelaciona como un proceso core del negocio en sí. Por ejemplo, en un banco mi proceso core es sacar tarjetas de crédito, entonces el subproceso sería el envío de las tarjetas a las personas y eso es core del negocio. ¿Qué involucra eso? las personas, el envío, la recepción, la verificación, etc.

Pero, en las instituciones públicas, el determinar un subproceso implica el tener que reunirse con las distintas áreas y eso conlleva un problema el hacer un problema core como tal. Ya que encima que la gente no está bien inmiscuida o bien metida por lo que resulta más difícil hacerlo. Entonces, para ir haciendo un proceso multiplicador como proceso inicial para que se pueda replicar, la idea que se está tomando es la de hacer un proceso TI que le sea más amigable y a su vez que tenga mayor repercusión, yo creo que es un tema que se puede sustentar nosotros, porque es un tema que lo conocemos, nos estamos dando cuenta que esa es la mejor manera.

Vino una empresa la vez pasada y me dijeron: "los procesos, el core del negocio, hay que realizar una tormenta de ideas, etc. esa es la mejor manera". Y yo le pregunté: ¿Y el centro de datos? "No, eso no se recomienda, porque el centro de datos es de

apoyo". Entonces uno se pregunta: ¿Qué se puede decir de la ONP, Qué se puede decir de la ONPE, Qué se puede decir de INDECOPI? ¿Están mal acaso? No están mal.

Al final ¿cuál es la realidad? Que nosotros, como estamos más metidos en este tema, tenemos que atacar un problema que abarque lo más posible y que lo conozcamos, para que una vez que nosotros hagamos todos los pasos para la implementación y, luego, ese proceso va a ir replicado a las demás dependencias.

Yo: ¿Cree que es importante que participe algún área que ve procesos en la institución?
E: Si, es muy importante. Es la materia prima en la entidad. Normalmente esto lo ve planificación o también el área de riesgos, si es que lo hay, aunque en las instituciones públicas esa área no hay. Pero también podría ser el área de calidad.

Yo: ¿Pero cree que estas áreas especializadas en procesos entiendan como es el funcionamiento del centro de datos?
E: Lo que pasa es que para el tema de implementación de sistemas de seguridad de la información, se requiere una cierta cantidad de información como visión, misión, procesos. Toda esa información que nos la da la ONGEI en formatos tienes que recogerla de algún lugar y si no está, tienes que hacer ese proceso. Entonces, si hay un área de procesos mucho mejor, porque con ellos puedes trabajar y asi determinar cuál es el mejor proceso para comenzar. Ahora, si al final se decide iniciar el SGSI con la Oficina de TI, si bien es cierto el de procesos no va a entender mucho, pero si te va a apoyar totalmente en el detalle de los procesos y su mejoramiento. Es un aliado.

Por ejemplo, en el MINTRA tenía conformado el Comité de Gestión y el Comité Técnico de Seguridad de Información, tenía el Documento de Políticas, con resoluciones, con todo oficializado. También tenía el Alcance, que ya estaba amarrado con un análisis de riesgos y el Plan de Contingencias a medias. Había todo eso. Pero, el Alcance seleccionado era uno a nivel de macro proceso, era un proceso inmenso. Es decir, a pesar de tener todos los requisitos solicitados en la norma, el proceso era inmanejable.

Un sistema de gestión de seguridad de la información es un subproceso que va a tener un efecto multiplicador en el tiempo. Si el proceso es muy grande no se contará muchas veces con el personal necesario y del apoyo de ellos, además de la cantidad de aplicaciones que maneja, de personal, etc. Por eso, es mejor partir de algo más modesto pero que sea significativo hacia algo más grande después. Tienes que tener mucho cuidado al seleccionar tu Alcance.

Yo: ¿Cómo percibe Ud. la cultura organizacional respecto del cumplimiento del SGSI en su institución?
E: La cultura organizacional respecto al cumplimiento del SGSI en mi institución, se encuentra en una etapa de transición. La Oficina de Tecnologías de Información (OTI), viene realizando denodados esfuerzos para obtener el apoyo de la Alta Dirección y de los demás funcionarios, a fin de que comprendan la importancia de implementar el SGSI en la institución; pero hasta el momento ha sido mínimo.

La OTI viene elaborando la política de seguridad de la información, el alcance de SGSI, el plan de sensibilización al personal, entre otros. Cabe destacar, que este plan de sensibilización permitirá conocer y crear conciencia respecto a la seguridad de la información.

Yo: ¿Tienen definido o están utilizando alguna metodología de riesgos para la implementación del SGSI en su institución?
E: Aún no hemos elaborado un análisis de riesgos, pero la que utilizaremos en su momento, será una metodología propia.

Yo: ¿Qué factores cree Ud. que impactan o impiden la implementación completa del SGSI en las instituciones del Estado Peruano (s/ la actual NTP 27001)?
E: Según mi experiencia laboral y profesional existen tres (03) aspectos que impactan en la implementación del SGSI:

1. No se tiene el decidido apoyo de la Alta Dirección para la implementación del SGSI en la mayoría de las instituciones. Esto se debe, por el desconocimiento de los peligros y consecuencias de la no implementación del SGSI en las instituciones y su vez también por los constantes cambios de gestión que suceden a menudo.

2. No existe un área de Seguridad de la Información que dependa directamente de la Alta Dirección, que sea liderada por el Oficial de Seguridad de la Información y que no tenga que ver con el área de Tecnologías de la Información de la institución. Sería recomendable que tenga su presupuesto y que esté considerado en el ROF y MOF institucional.

3. El cargo de Oficial de Seguridad de la Información, recae en un personal sin experiencia.
   En la mayoría de los casos este cargo lo asume el Jefe o algún personal de TI, los mismos que por tener funciones ya asignadas por el cargo que desempeñan, se les hace difícil realizar las actividades concernientes a la implementación del SGSI. En dicho cargo se necesita personal con experiencia y capacitación necesaria, a fin de que sea el interlocutor entre la Alta Dirección y las demás dependencias de la institución y además esté a tiempo completo para realizar la implementación del SGSI.

ANEXO 9: TRANSCRIPCION DE LA 2da. ENTREVISTA

La entrevista está dividida en 03 partes:

La primera tiene que ver con la parte más técnica, es decir con la experiencia laboral y personal que Ud. tenga con respecto a la seguridad de información. Una segunda parte normativa, que son preguntas referidas a la misma norma y con la ONGEI misma que es el ente que norma este proyecto. Y una tercera parte operativa, que son preguntas del SGSI en su Institución, es aquí donde desarrollaremos más profundamente el tema de la tesis de investigación

Entonces, respecto de la Parte Técnica:

Yo: Referente a la experiencia laboral y personal, ¿Cómo define Ud. lo que es un Sistema de Gestión de Seguridad de Información?
E: Bueno, un SGSI -como su nombre lo dice- es un conjunto de elementos diversos que permiten trabajar de forma interrelacionada para cumplir ciertos objetivos. En este caso, cuando hablamos de un SGSI estamos hablando de la Confidencialidad, Disponibilidad, Integridad. Esto quiere decir que un SGSI tiene que estar dentro de un Alcance de la Organización definido en un momento determinado por las instancias correspondientes.

Yo: Mencióneme Ud. su experiencia profesional o personal en la Seguridad de la Información.
E: Yo he trabajado en diferentes entidades del sistema financiero y en empresas tanto públicas como privadas, donde siempre he podido ver temas de implementación de seguridad de la información relacionadas por ejemplo con la Superintendencia de Banca y Seguros, y también con la misma norma (NTP) que en su momento se le conoció como la 17799; sin embargo, con el transcurrir del tiempo, esta norma ha ido evolucionando. Mi experiencia, dentro de las empresas privadas, las transnacionales las que, de alguna otra forma, tienen otra visión, otra casuística de cómo ven la seguridad de la información.

Yo: ¿Tiene Ud. alguna certificación o especialidad en seguridad de información?
E: Correcto. Tengo las certificaciones de ISACA: CISA, CISM y CRISC. Tengo también una certificación del DRI: la ABCP y también tengo otras certificaciones menores como: ITIL, COBIT Foundations, ISO 20000. Están relacionadas.

Yo: ¿Pertenece (o ha pertenecido) a alguna asociación vinculada a la seguridad de información)?
E: Si. Pertenezco a ISACA (*) y en este momento también pertenezco al DRI (**) y también al PMI (***)

Respecto de la Parte Normativa, se pretende ver la dimensión del proyecto en sí:

Yo: Para Ud. ¿Qué viene a ser la Norma Técnica de Seguridad ISO 27001 y qué papel cumple la ONGEI en esta norma?
E: Bueno, la norma es un conjunto de prácticas que pueden ser aplicados en una organización para salvaguardar su activo principal, que en este caso, es la

información. Cuando hablamos qué papel cumple la ONGEI, entiendo desde el punto de vista de la Presidencia del Consejo de Ministros, es un ente rector que se encarga de centralizar toda la documentación normativa y también, en algunos casos, la dirección consultiva en la implementación de esta norma, básicamente es eso.

Yo: ¿Qué objetivos busca el Estado Peruano con la implementación de esta norma?
E: El objetivo principal es proteger la información de nuestro país. Justamente nuestro país, si bien es cierto, somos un país que no estamos todavía a un nivel de un país desarrollado, donde hay grandes organizaciones que se dedican a este tema; sin embargo, nuestro país está en línea a esta norma técnica que salvaguarda la información y que es considerada en estos tiempos como el activo más importante de una organización.

Estamos viendo pues que hemos pasado de una era de producción a una era de la información y ahora estamos pasando a una era del conocimiento. Entonces, todo ese tránsito que hemos tenido y que estamos viviendo, conlleva a pensar y a repensar que la información realmente, en algún momento, va a tomar un rol muy estratégico en las decisiones de nuestro país.

Sin embargo, podemos ver ya hoy los grandes incidentes que están ocurriendo a nivel mundial y que están afectando países completos, están afectando la imagen, y lo cual no estaríamos muy lejos de que pueda suceder esto en nuestro país. Por esa razón considero que es muy importante implementar estos sistemas de gestión en nuestro país, y que mejor que en nuestras instituciones públicas.

Yo: ¿Tiene Ud. conocimiento de normas técnicas anteriores a la actual (a la 27001)?
E: Efectivamente. Mi experiencia justamente radica en la primera versión. Esto tiene una larga historia desde el estándar británico la BS 7799, luego salió la ISO 17799 y luego salió la 27001, etc. Y podríamos hablar de toda una gama de normas de la línea 17799 y de la familia 27000, en donde muchas de ellas han ido evolucionando conforme la tecnología y la sociedad lo han venido haciendo.

Yo: ¿Ud. cree que estas normas anteriores con la norma actual han mejorado la forma de trabajo en la Organización?
E: Más que mejorado, ha cambiado la óptica. Osea, todas las normas han sido válidas en su momento. ¿Porque? Porque en su momento hubo una cierta tecnología. No puedo comparar la tecnología que hubo hace 03 años con respecto a la que existe hoy. Hace 03 años quizá no habría algunos riesgos que hoy existen.

Se necesitaban menos controles, se necesitaban normas que no eran tan exhaustivas. Sin embargo hoy tenemos la tecnología y se ha incrementado fuertemente el hardware. Existen dispositivos que cumplen papeles de grandes servidores conlleva a que los controles se vuelvan más sofisticados y las normas también avancen en ese sentido.

Yo: Incluso antes, no todos tenían acceso a un Smartphone, celulares con grabadoras; cosas que todo el mundo tiene hoy, por lo que la información debería estar más protegida que antes, debe tener más controles ¿verdad?

E: Efectivamente. Cuando hablamos de hace muy poco, hace 10 años atrás, no existían incluso algunas carreras que hoy conocemos: como el ingeniero de seguridad informática, el oficial de seguridad de la información. Antes simplemente hablábamos de la gerencia de tecnología y sus riesgos.
Las grandes firmas que hoy existen en el mundo, todavía se puede apreciar como grandes ramas de servicios lo que es riesgos de tecnología, riesgos de servicios; pero eso ha evolucionado. Hoy podemos apreciar que las grandes firmas tienen segmentos exclusivos para brindar servicios de seguridad de la Información, continuidad de negocios, Gobierno de Tecnologías de la Información. Son temas que han evolucionado con el tiempo.

Yo: ¿Sabe si con la 27001, con esta norma actual, ya hay empresas que han implementado con éxito? E: Si. Tengo entendido que en nuestro país por ejemplo tenemos el caso de la ONP, INDECOPI donde he podido ver de cerca las experiencias que han tenido, y en el caso de RENIEC de igual forma donde he vivido en carne propia el proceso de certificación de la ISO 27001.

Yo: ¿Qué factores cree que están afectando la implementación de la norma (ISO 27001) en el Estado Peruano?
E: Una de las razones principales es la falta de apoyo de la Alta Dirección. Generalmente este tema la Alta Dirección lo ve como un tema informático, lo ve como un tema sui generis que no tiene mayor importancia por desconocimiento.

En otros casos, puedo mencionar la falta de profesionales especializados en este tema, que es muy escaso en nuestro país. Generalmente, los pocos que existen están trabajando y no se abastecen en su totalidad para poder apoyar o implementar en estos temas.

También puedo rescatar el hecho de los costos. Muchos creen que implementar un sistema de gestión a la larga es implementar controles y estos controles -en el fondo- es dinero para la empresa. Muchas empresas no tienen el presupuesto necesario o porque no lo han pedido, y le resulta difícil implementar en una institución pública. Por ejemplo, un DLS, es decir un software que te identifique la fuga de información ¿es caro? Sí, es caro. Un IdM, Identity Management, que pueda centralizar la gestión de accesos, es caro también. Pero la pregunta es: ¿realmente nos sirve, ayuda a la Organización? Entonces, son temas que una organización, a través de la Alta Dirección, tiene que evaluar previamente que es lo que realmente va a obtener como ventaja.

Muchos piensan que la certificación es una medalla más, pero debemos recordar que no es así, sino que en el fondo es un esfuerzo común y difícil para todos los que implementan una certificación y donde se está tratando de proteger la información (y digo tratando porque no se llega a proteger totalmente) y que se minimice la mayor cantidad de riesgos.

Yo: Esto indica que no se toma todavía la Seguridad de Información a nivel de toda la organización sino de un proceso, se podría decir por partes o de a pocos ¿Qué piensa Ud.?

E: Es un tema importante el que tocas, porque si bien es cierto que la R.M. 129, vigente en este momento, menciona simplemente el uso obligatorio de la norma en el Alcance que defina la organización, no es claro. Entonces, en el Alcance uno puede definir un área, un proceso, un sub-proceso o toda la institución y eso es justamente quizás uno de los errores más comunes que se está manejando, porque en realidad la Seguridad se debe implementar a nivel institucional.

Ahora, claro que siempre contrastando contra el mapa de riesgo que se tenga. Porque, si yo no tengo o no conozco a ciencia cierta mi mapa de riesgo de todos los procesos de una organización, ¿cómo podría decir que lo voy a implementar aquí y en el otro no? Entonces, tiene que haber un estudio preliminar para poder determinar el alcance real y que esto se alinee a los objetivos estratégicos que busca la Organización.

Yo: Viéndolo a nivel de todo el Estado, es decir de todas las instituciones del Estado, creo que se hace más difícil su implementación ¿Es así?
E: Si. Se hace más difícil y además se comprende que las instituciones se manejan de manera política y, en realidad, las personas somos pasajeras. En muchos casos, se puede apreciar que se hace por cumplir un cierto objetivo A o B, pero más allá de estos objetivos debería estar plasmado en un objetivo como país. Así como se tienen otros objetivos de país sobre la pobreza o sobre el desarrollo económico, debería haber un objetivo similar en lo que respecta a cuidar y proteger nuestra información como país y que mejor en nuestras instituciones públicas.

Yo: Tocando un tema que tocó anteriormente respecto de la rotación de los especialistas en las diferentes instituciones ¿Hay documentación que se deja al respecto. Es decir, si yo voy a una institución puedo continuar o debo empezar de cero?
E: Bueno, en realidad va a depender del control interno que se maneje en cada organización, no se puede generalizar. El control interno establece las políticas, procedimientos e instrucciones para darle continuidad a las actividades que se desarrollan en una institución, unas lo tienen más desarrolladas que otras. ¿La pregunta es? ¿Realmente se cumple el control interno?

Específicamente si vemos para Seguridad de Información, ¿Existen procedimientos -como mencionas-que permitan verificar la continuidad? Porque esto va más allá de la jefatura, va a un nivel estratégico que tiene que ver con la Alta Dirección.

Yo: Incluso si fuera una Política de Estado -a nivel del Gobierno Central- ¿No se podría ver más esta continuidad?
E: En realidad, este tema de la continuidad tiene que ver con la gestión del conocimiento, porque no solamente lo enfoco para Seguridad sino si hablamos de términos generales para toda la organización van a haber procesos claves y van a haber procesos de soporte pero que también son claves para que pueda operar. Y dentro de estos procesos vamos a encontrar ciertos elementos que son fundamentales que tienen que estar identificados que tiene que tener una continuidad y no deberían pararse y que deberían gestionarse y administrarse conforme se ha establecido.

Entonces, para eso hay que tener varias cosas que se tienen que implementar. Por ejemplo, Uno es que el control interno esté bien implantado en una organización. Segundo, la continuidad de negocios que tienen que ver con la seguridad de

información. Ambos tienen que conversar. Otro elemento es el Gobierno de las Tecnologías de la Información y las Comunicaciones que también deberían de conversar. Es decir que son varios frentes de una organización que tienen que trabajar en paralelo para lograr un frente común.

Yo: Hablando de un frente común, ¿Cree Ud. que la ONGEI debería cumplir un papel más fuerte o está bien cómo lo viene haciendo actualmente? Es un líder de la seguridad de la información?
E: Personalmente, pienso que la ONGEI ha cumplido su papel hasta cierto punto pero falta mejorar muchas cosas. Por ejemplo, debería tener un set de profesionales consultores que le den soporte a todas las instituciones públicas.

Actualmente, las instituciones públicas se están disparando por su lado; Cada una busca sus consultores, cada una busca contratar una empresa que lo ayude a implementar. Todas lo hacen a su manera, pero no hay un ente que diga: Miren señores, yo tengo mis especialistas, pueden usarlos. Si Uds. quieren contratar estos son las referencias que pueden tomar, aquí tenemos una base de conocimientos. Esto ayudaría enormemente pienso a que cualquier entidad nacional, local y regional puedan implementar esta norma y que mejor que contar con un staff de especialistas peruanos y extranjeros con conocimiento en este tema.

Respecto de la Parte Institucional:

Yo: ¿Qué beneficios trae a su institución la implementación de esta norma?
La norma de seguridad de la información definitivamente ayuda a cumplir con los objetivos estratégicos que se ha trazado la institución. Dentro de estos objetivos está la de brindar servicios de calidad, brindar servicios relacionados con tecnología; por tanto, para brindar este tipo de servicios, lógicamente uno tiene que pensar en la seguridad, ya que la seguridad hoy por hoy cumple un rol importante, y con mucho más razón aún ya que nuestra institución administra la base de datos de nuestro país con más de 28 millones de registros se custodian aquí. Por tanto, el hecho solamente de que un registro no esté protegido nos podría generar muchas consecuencias como país y a nuestra seguridad nacional. Entonces, para nosotros, el tema de seguridad de la información es un pilar muy importante porque es parte de nuestro negocio.

Esta institución, si bien se ha certificado en un proceso, en realidad tenemos 05 procesos claves, de los cuales en este momento nos encontramos implementando en 02 procesos más: Identificación de ciudadanos y Registros civiles.

Yo: ¿Uds. hace cuánto tiempo iniciaron su implementación?
E: Bueno, este proyecto se inició más o menos hace 2 años. Esto proyecto nace a consecuencia del proceso de certificación digital que lleva a cabo gran parte de lo que es el Gobierno Electrónico con la implementación del DNI Electrónico, nos abre las puertas para el uso de los certificados digitales. En ese marco, la institución como país está buscando hacer posible de que nuestros DNI´s electrónicos tengan uso a nivel internacional; eso quiere decir que, si en el futuro llegáramos a certificarnos a instancias superiores, nuestro DNI tendría validez en cualquier país del mundo.

Actualmente, si bien es cierto nos hemos certificado, todavía no podemos hacer operaciones a nivel internacional. No tiene validez. Cualquier persona que tenga un

DNI electrónico, va a poder firmar electrónicamente; sin embargo, sus operaciones todavía no tienen validez a nivel internacional, sus certificados aún no son reconocidos como otras grandes instituciones que ya existen en nuestro país.

Este camino de la validez a nivel internacional requieren pasos, uno de ellos era obtener la certificación de la ISO 27001. Entonces, hay todo un plan estratégico que la institución está implementando para que en el futuro no muy lejano, estos DNIs tengan validez internacional.

Yo: Cuándo Uds. tuvieron que empezar con la implementación del Sistema de Gestión de Seguridad de Información, ¿Por dónde comenzaron? ¿Cómo definieron el Alcance más importante?
E: El tema del Alcance siempre parte del objetivo estratégico que requiere la organización. Hay que partir de los servicios que requiere una organización; Por ejemplo, nosotros entregamos DNIs, actas de nacimiento, actas de defunción, etc. Ese es nuestro negocio, a eso nos dedicamos. Entonces, yo debo proteger primero lo que yo vendo. Para eso tengo que identificar los procesos que soportan estos servicios que dan vida a esta institución, la cual ha sido creada mediante una Ley.

La Ley dice bien claro cuáles son las funciones que va a ejecutar la institución y sobre eso se soportan los servicios y sobre estos están los procesos. Y uno de los procesos muy importantes es la Certificación Digital, que es el proceso que está certificado. Tan igual como proceso hay otros procesos más: Certificación de Ciudadanos, Registros Civiles, Padrón Electoral y Otorgamiento de Servicios. Son 05 procesos claves que la institución los tiene así calificados. Sin embargo, por la envergadura de las operaciones y la perspectiva hacia el futuro, en este momento, los procesos más importantes son: el de Certificación Digital, Identificación de Ciudadanos y Registros Civiles.

Yo: Para la identificación de un proceso esencial de la Institución ¿Cree Ud. que es necesario tener desarrollado un tema de gestión de calidad de procesos?
E: Acá hay 2 temas que debemos diferenciar bien: Se quiere implementar o se quiere certificar. ¿O se quieren las dos cosas? Por ejemplo, las instituciones financieras no están certificadas, sin embargo han implementado su sistema de gestión seguridad de información. No están certificadas pero cumplen -yo aseguraría- en mayor grado que aquellas que están certificadas.

Entonces, debemos tener cuidado de que no necesariamente una entidad que está certificada se podría decir que está implementada al 100%.

Yo: Pero para definir un Alcance ¿Es necesario que se tenga bien definido el tema de procesos?
E: No, no es necesario. Ya que un Alcance se puede ver de diferentes ángulos.

Yo: Le pregunto esto porque, normalmente en el Estado, un problema recurrente es el mapa de procesos (MAPRO) de la mayoría de las instituciones, el cual está desactualizado con mapros del 2002 o del 2005 e incluso ya las funciones han cambiado. Entonces, ¿Cómo se va a definir un Alcance de la organización, si tal vez ese proceso no está bien definido?
E: Lo que sucede es que debemos diferenciar dos cosas acá:

Voy a ir por la 1ra. parte de la norma, con respecto al Alcance te dice bien claro que uno lo puede ver desde el punto de vista de procesos, áreas, secciones, actividades. Por tanto, uno tiene la libertad de poder determinar dicho Alcance.

Ahora vamos a la 2da. parte, ¿Porqué para una institución pública sería importante desde el punto de vista de procesos?
Porque cuando hablamos de una institución pública, está amarrada a otras normas. Ahora, por ejemplo, tenemos la Ley Servir, la cual te habla a nivel de procesos.

Entonces, no podemos cerrarnos simplemente a lo que nos diga la norma, sino que van a ir acoplándose otras normas que nos obliga a que tomemos, en algunos casos, por procesos.

En el caso puntual de ésta institución, se ha tomado por procesos, porque ya en su momento se han definido -en una anterior gestión- los procesos clave que ya existían en esta institución.

Yo: ¿Tengo entendido que Uds. desarrollaron el sistema de gestión de calidad en el 2001?
E: Efectivamente. Justo este sistema de gestión de calidad de la institución ha ganado muchos premios y, en este momento, entiendo que hace poco nos hemos re-certificado en uno de los procesos en ISO 9000. Esto ha permitido administrar una cultura sobre los sistemas de gestión.

Muchos de los documentos de este sistema de gestión de la ISO 9001, son comunes para la ISO 27001 y eso ayuda. Estos documentos comunes, en algunos casos varían, en lo mínimo, pero cumplen el mismo rol.

Yo: ¿Y Uds. recibieron -para este sistema de gestión ISO 9001- algún tipo de capacitación externa, tercerización o Uds. mismos lo implementaron?
E: Esto fue desarrollado en el 2006, y yo no estaba aún laborando aquí en aquellos años. Pero, por lo que me han referido, efectivamente mucho se han ayudado con consultoras. Es que si hablamos del 2005, 2006, 2007 o 2008 pues esto era algo que no se conocía y en ese tiempo había muchas consultoras especializadas que venían de México, por ejemplo. En Perú, recién se estaban instalando algunas y esto ha ido madurando en el tiempo.

Yo: ¿En su institución han tenido apoyo de la Alta Dirección, habida cuenta de que Uds. ya vienen implementando el SGSI en varios procesos?
E: Totalmente ha habido dicho apoyo por la Alta Dirección. Esto se puede evidenciar desde el momento del acta de constitución de un proyecto de esta naturaleza, quien lo preside es el jefe nacional, que es la entidad máxima de esta Institución.

Yo: Tengo entendido también que la oficina de seguridad de información, no está dentro del área de TI. ¿Qué puede decir al respecto?
E: Efectivamente, la oficina de seguridad de la información está en otra área, en la oficina de seguridad y defensa nacional, el cual es un órgano de nivel asesor y que reporta directamente a la alta dirección es decir al jefe nacional.

Yo: ¿Considera Ud. que está bien así o que debería estar tal vez más cerca del área de TI?
E: Lo que sucede es que eso va a depender del grado de la cultura que exista en una organización. Conozco casos de entidades privadas donde la gestión de la seguridad de información lo maneja desde el área de la Gerencia de TI. Funciona, pero eso depende de la cultura.

En el caso de las entidades públicas, lo más recomendable es que no pertenezca a las Gerencias de TI porque de alguna forma se convierten en juez y parte, y eso es lo que uno debe evitar. Este tipo de áreas deben trabajar independientemente del área de tecnología pero no pueden estar supeditadas a un gerente de TI que les pueda decir en algún momento que cosas van y que cosas no.

Yo: ¿Considera Ud. que la Alta Dirección tiene claro lo que es un SGSI?
E: En el caso de la Institución donde estoy si lo tienen claro y le dan la importancia debida. Por ello es que ahora nos encontramos implementándolo en 02 procesos más.

Yo: ¿Cómo está conformada la organización del SGSI en su Institución?
E: Tenemos un Comité de Gestión de Seguridad de la Información que está integrado por el Jefe Nacional, por la Secretaría General y el Gerente General, que son los entes máximos de la Institución. Este comité de gestión se encarga de ver aspectos generales del sistema de gestión de seguridad de la información.

La organización entonces está compuesta por: el comité de gestión, el oficial de seguridad y sus coordinadores de seguridad de la información. En cada área de la Institución existe un coordinador de la seguridad de información.

Yo: Esa forma de organización ¿Es un nuevo aspecto o ya lo han implementado de otras organizaciones grandes?
E: Lo que sucede es que nosotros hemos aplicado la estrategia de la descentralización.

Un SGSI se puede implementar de varias formas: Se puede implementar de forma centralizada y en forma descentralizada.

De forma centralizada es: *Yo pongo un oficial de seguridad y pongo un pool de analistas que vean la seguridad de toda la institución*.
La otra forma de implementarlo es la descentralizada: *Tener un oficial y tener coordinadores de seguridad en cada una de las áreas de la organización, por más chica que sea esta*. *Estos coordinadores son como mini oficiales de seguridad*.

Estos coordinadores en algunos casos -dependiendo de la complejidad del proceso- están dedicados a full- time y en otros casos a part-time. Además, deben cumplir con un perfil mínimo de especialistas en seguridad, aparte tienen funciones y además se les da una capacitación, una inducción y se les hace una evaluación. Todo esto es un proceso de aprendizaje continuo.

Yo: ¿Y toda esta organización parte del apoyo de la Alta Dirección?
E: Así es, cuenta con el apoyo total de la Alta Dirección.

Yo: Yendo al tema de la capacitación, tengo entendido que hay una capacitación técnica y otra para la organización, ¿Cómo es en el caso de su institución?
E: Tenemos un programa de capacitación que están dirigidos a diferentes segmentos. Por ejemplo, hay capacitaciones dirigidas a la Alta Dirección, capacitaciones dirigidas a los coordinadores de seguridad de la información y capacitaciones dirigidas a todo el personal de la institución. Esto debido a que el lenguaje debe ser diferente, ya que no haría bien en hablarle a un registrador de unos temas de seguridad de la información que no son de su interés, sino más bien de los tipos de incidentes que le podrían ocurrir a él, qué tipo de riesgo puede detectar; mientras que con la Alta Dirección estaremos más enfocados en las estrategias, como por ejemplo, cuáles serían las estrategias a utilizar con los proveedores de seguridad de la información, sobre los acuerdos de confidencialidad, sobre la seguridad informática, etc.
Entiéndase que esto es una especie de nivel de madurez, es un proceso de "evangelización" como yo lo llamo. Si vamos a iniciar con una organización que nunca ha implementado seguridad de la información, definitivamente el trabajo va a ser más arduo y el nivel de complejidad tiene que iniciarse de lo más simple a lo más complejo, entonces esto va a depender del nivel de madurez que se tenga en el campo de la seguridad de información.

Yo: Eso es por el tema de la organización, ¿Y por el tema técnico, es decir por parte de los especialistas que ven este tema en su organización, también hay capacitaciones?
E: Efectivamente, si hay capacitaciones. Tengo entendido que la gerencia de TI tiene un equipo de seguridad informática, se han certificado; están llevando un curso de especialización en el SGSI, específicamente en lead implementer, lead auditor, ISO fundation 27001 y también aspectos técnicos de las actividades propias que ello desarrollan.

Yo: Y como Oficial de Seguridad de su entidad, ¿Ud. también recibe capacitaciones?
E: Si llevo capacitaciones pero en forma personal, en ese tema estamos trabajando todavía. Es que hay un tema que debemos entender: Si tienes tiempo revisa todos los ROF y verás que el Oficial de Seguridad no existe como un rol (en dicho ROF) como tantos otros roles existentes en el Estado.
Generalmente, este rol muchas empresas lo toman como algo momentáneo, que mientras implementemos el ISO 27000, lo contratamos y luego una vez que termine, termina el proyecto y todos se van. Piensan que es un producto que se compra y se vende, entonces en ese tema se está trabajando bastante en la institución donde estoy para que esto se incluya como algo permanente.
Sugiero que hagas una revisión de los demás ROF y te vas a dar cuenta que no existe un rol de oficial de seguridad de información.

Yo: ¿Hay presupuesto como para desarrollar el SGSI o hay problemas presupuestales?
E: En la institución en la que estoy actualmente se ha sabido sustentar. Presupuesto entiendo que si hay; sin embargo, todavía existen dificultades en el sentido de que, como este cargo es bien especializado y bien técnico, las gerencias de RR.HH. todavía no lo tienen claro. Piensan que el rol de oficial de seguridad de información

debe asumir cualquier persona. Esta mala interpretación involucra a ponerle cualquier monto de salario y poder designar a cualquier persona. Entonces, eso puede llevar a errores graves que todavía están en proceso de maduración.

Yo: Teniendo en cuenta que ya se tiene implementado el SGSI en su institución ¿Cómo se desarrolla el tema de la cultura organizacional hacia el personal para que lo aplique en la misma?

E: Acá estamos hablando de la concienciación. El problema de concienciación involucra muchos canales. El simple hecho de que uno pueda publicar un folleto donde te indique por ejemplo que tengas cuidado al dar un clic o no abrir cualquier correo, ya estamos hablando de concienciación.

Entonces, en la institución existen muchos canales, utilizando los medios tecnológicos, las capacitaciones y las consultas directas que recibimos. Generalmente, nosotros estamos constantemente en contacto con nuestros coordinadores y con el personal. Con los gerentes hacemos, en algunos casos, capacitaciones mensuales o bimensuales. Estamos en ese proceso de evangelización.

En algunos puntos nos ponemos en su realidad y nos preguntamos, ¿Qué podría pasarles, en temas de seguridad de la información, para que ellos tomen conciencia?

Por ejemplo, la semana pasada tuvimos una capacitación en un área de registros y estuvieron presentes digitadores que ingresan data. Entonces, la pregunta que uno se haría es: ¿En un digitador, qué riesgo de seguridad de la información puede haber? Si uno entra a analizar las funciones que realiza, uno se puede percatar de que puede haber errores en el ingreso de la información y por ahí puede haber brechas importantes que quizás resulten en fraudes. Ese tipo de aspectos uno va conversando con el personal, va comunicándose y es ese mismo personal el que participa de estos talleres donde se les da las herramientas para que a ellos mismos identifiquen ese tipo de problemas que pueda ocurrir y puedan tratarlo oportunamente.

Yo: Uds. tienen una institución con sedes en todo el país, ¿mantienen ese mismo esquema de coordinadores de seguridad de información a nivel nacional o solo es en la sede central?

E: En este momento no tenemos a nivel de provincia sino a nivel de jefaturas en gerencias. Si estamos empezando a extenderlo pero, como te mencionaba antes, este es un proceso de maduración; conforme vamos a ir ampliando los procesos que van a estar implementados, tiene que haber también un área que le de soporte.

Si se quiere ampliar esto a nivel nacional, de hecho va a involucrar quizás incluir algunos cargos más en el área de seguridad de la información, y esto lleva a un presupuesto adicional. En este momento, si bien es cierto no es nuestra prioridad, porque estamos implementando dos procesos que no incluyen generalmente un alcance nacional; sin embargo, en el corto plazo si lo tenemos en mente implementar a ese nivel.

Yo: ¿Podría darse que cada coordinador de sus propias capacitaciones o éstas se dan para todos en conjunto?

E: Se podría dar, pero recuerda que los coordinadores aún están en un proceso de aprendizaje. Entonces correríamos el gran riesgo de que se pueda dar en este momento una mala capacitación y, por ende, se podrían interpretar mal algunos controles que quisiéramos difundir. Nosotros estamos por ahora centralizando todo, hasta que lleguemos a un nivel de grado de certeza de estar convencidos de que los

coordinadores estén debidamente capacitados. Y en ese momento, que descentralizaremos para que ellos difundan en sus demás áreas más adelante.

Yo: ¿Qué metodología de riesgos han implementado Uds.?
E: En un inicio teníamos implementada la ISO 27002, la de la misma norma, que estaba orientada a activos. Sin embargo, con la ISO 27001:2013 sabemos que esto ha cambiado. Ahora la metodología de evaluación de riesgos de esta nueva norma te la deja abierta, es decir que ya no se enfoca necesariamente en los activos, sino más bien estamos hablando de un riesgo empresarial.

Por tanto, ahora se habla de metodologías como la de COSO, de IT Risk, del Estándar Australiano, de Magerit; en realidad, no hay fórmula. Sin embargo, no debemos perder la visión de que el riesgo debe estar bien identificado. Es decir, que ese riesgo existe, es potencial, se podría materializar y afectaría finalmente a los objetivos de la institución.

Entonces, en este momento la metodología que tenemos es una metodología híbrida que incluye varias que se ha adaptado a la realidad de la institución, con la finalidad de desarrollar los requerimientos de la ISO 27001:2013 y cumplir con la parte técnica que nos pide la norma.

Yo: Hablando de este tema ¿Cómo Uds. están piensan adaptar el proceso de SGSI ya implementado a la nueva norma ISO 27001:2013? Y además, los procesos que vienen trabajando ¿van a contemplar esta nueva norma?
E: En este momento venimos trabajando con la nueva norma que es la NTP-ISO/IEC 27001:2014. Además, todos los documentos o registros de información que tenemos del proceso certificado, ya nos encontramos adecuándolo a la nueva versión.
En realidad no hay cambios enormes porque, en algunos aspectos, la 27001:2005 era incluso más exhaustiva. Sin embargo, la versión actual te abre muchas posibilidades que no necesariamente hay que hacer una reingeniería como se dice. Estamos haciendo cambios mínimos, que en realidad no son grandes cambios que vamos a tener que modificar todo lo realizado. Es más acomodable, más manejable.

Yo: Para terminar ¿Qué factores considera Ud. no están permitiendo la implementación del SGSI en el Estado?
E: Existen varios factores:
El primero es el factor político, en el cual muchas personas pueden estar ingresando a laborar en seguridad de información y desconocen el tema, no son especialistas.
El segundo factor, es la falta de profesionales especializados en este tema tanto a nivel público como privado.
Un tercer factor para mí que está influenciando sería el presupuesto. Muchas instituciones no cuentan con presupuesto, puesto que no solo es implementarlo sino también hay que darle mantenimiento. Entonces, algo que inicias hoy no es algo que va a acabar el otro año, sino que esto ya no acaba sino que se mantiene permanente en el tiempo. Por tanto, hay que ver bien este tema. Cuando uno quiere implementar un sistema de gestión, no se trata solamente de decir cuánto me va a costar el proyecto, sino que hay que contemplar la implementación más el costo del mantenimiento y esto incluye poner un equipo de personas nuevo: un oficial, un analista de seguridad, y que formen parte de la institución para su mantenimiento.
Por otro lado, muchas instituciones piensan que cuando hablamos de seguridad de la información estamos hablando de tecnología. Es decir, que hay una falta de cultura

del SGSI que tienen en la Alta Dirección. Piensan que hay que comprar tal o cual software, tal herramienta; pero esto va mucho más allá que un elemento.
El siguiente factor podría ser la definición de los procesos. El establecimiento de procesos de una organización que muchas instituciones públicas no lo tiene o que van cambiando en el tiempo y no se actualizan.
Otro factor sería también la rotación del personal, donde en las instituciones públicas muy poca es la que está en planilla. Generalmente casi todos son contratados como CAS o servicio de terceros. Entonces, no hay una continuidad del personal y, en muchos de los casos, la gente está pensando en su bienestar económico más que en el de la institución y del país.
Otro factor también que influye es el de los sueldos en la institución pública y que varían demasiado con respecto a los de las privadas. Entonces, es muy difícil que un buen profesional quiera trabajar en una institución pública.

Yo: Finalmente, ¿algo último que quiera agregar?
E: Bueno, comentarte que este tema de la seguridad de la información si bien es cierto es un tema prioritario para nuestro país; Sin embargo, no hay el apoyo político como país. Más allá de hablar de instituciones, esto debería ser una política de gobierno. Desarrollarse, como política, un plan de seguridad que permita implementar, verificar y controlar estos sistemas pero no a nivel institucional sino a nivel de país y que permitan optimizar el uso de los recursos, ya que, por ejemplo, se podría asegurar que una municipalidad de provincia tal vez esté gastando medio millón de soles en implementar un SGSI, y aquí en Lima, otra municipalidad lo esté implementando con veinte mil soles. Hay mucha diferencia en este tema. Entonces, tiene que haber una política clara que permita manejar y unificar esfuerzos.

(*) ISACA International, es la Asociación de Auditoría y Control de Sistemas de Información, conocida solo como ISACA, la cual brinda certificaciones CISA, CISM, CRISC, Cobit5, entre otras.

(**) DRI International (originalmente conocido como Disaster Recovery Institute) es un organismo de certificación de profesionales para la Gestión de la Continuidad de Negocio (BCM)

(***) El PMI, Project Management Institute, es una organización internacional que asocia a profesionales relacionados con la Gestión de Proyectos ofreciendo la certificación Profesional en Dirección de Proyectos (PMP)

ANEXO 10: TRANSCRIPCION DE LA 3ra. ENTREVISTA

La entrevista está dividida en 03 partes:

La primera tiene que ver con la parte más técnica, es decir con la experiencia laboral y personal que Ud. tenga con respecto a la seguridad de información. Una segunda parte normativa, que son preguntas referidas a la misma norma y con la ONGEI misma que es el ente que norma este proyecto. Y una tercera parte operativa, que son preguntas del SGSI en su Institución, es aquí donde desarrollaremos más profundamente el tema de la tesis de investigación

Entonces, respecto de la Parte Técnica:

Yo:¿Cómo define Ud. lo que es un Sistema de Gestión de Seguridad de Información?
E: Para mí, el SGSI es un conjunto de normas, políticas, procedimientos, directivas que le permite al Oficial de Seguridad poder gestionar, evaluar e implementar todo un sistema de información para la institución dado que este sistema no es sólo para informática. Por tanto, es un conjunto de políticas, normas y estándares que nos permite llevar a cabo toda la implementación del SGSI.

Yo: ¿Qué experiencia Ud. tiene profesional o personal con la Seguridad de Información?
E: Bueno, mi primera experiencia fue con una caja financiera donde se veía bastante la seguridad de la información, incluidos los backups a Hermes por ejemplo. Estamos hablando de hace 10 años, y donde se tenía toda una política de información de los clientes la cual no se puede perder. Ya desde allí venía aplicando las políticas, más no la norma. En las empresas privadas no hay esa norma, sino que la misma SBS tiene su propia política de riesgo, y ante ello, ellos mismos definen que tienes que tener esos parámetros. Entonces, por allí ya tenía esa experiencia.

Y es aquí donde impulso la implementación de la norma. Es más, cuando llegué no había nada del SGSI; por tanto, yo vengo a impulsar esta norma acá. Ahora ya se cuentan con una estrategia de seguridad de información. Es un tema que se viene avanzando.

Yo: ¿Ud. pertenece o ha pertenecido a alguna asociación vinculada a la Seguridad de Información?
E: No. Pero hay un comité de seguridad de la información que nos reúne ONGEI mensualmente. Esto más bien debería ser más frecuente y no cada vez que ellos lo requieren. Pienso que debería existir una normatividad quincenal o mensual para verificar los avances realizados y los problemas encontrados, lo cual no hay actualmente.

Respecto de la Parte Normativa, es decir del Proyecto en sí:

Yo: ¿Para Ud. qué es la NTP 27001 y qué papel cumple la ONGEI en la implementación de esta norma?

E: Bueno, la ONGEI sacó en el 2009 esta NTP donde obliga a 50 entidades a que implementen, inclusive con fechas de término incluyendo fases de avance.
Ellos se comprometieron incluso a brindar cursos de capacitación y únicamente hubieron 2 o 3 talleres. El papel que cumple es un órgano rector o coordinador pero no como debería ser, debería cumplir un rol más activo. Ellos tendrían que ser más proactivos.

Yo: ¿Qué objetivos cree que busca el Estado con la implementación de esta norma de seguridad de información?
E: Tengo entendido que lo que busca el Estado es que la información que manejan las entidades públicas sea bien manejada. Hay información que es reservada, confidencial y otra pública, los cuales deben manejarse en forma transparente. Hay información que no debe salir pero que lamentablemente sale y que incluso son de seguridad nacional.

Por ejemplo, en nuestro caso nosotros manejamos información confidencial que de salir hacia fuera podríamos hasta provocar un conflicto bélico. Eso es lo que nosotros manejamos, entonces tenemos que tener bastante resguardo de la información el grupo de personas que manejamos esto. Incluso, ahora mismo, tenemos una información privilegiada respecto de dónde están las coordenadas y el stock del banco de anchoveta, información que no podemos dar hasta que el gobierno haga oficial y levante la veda para que puedan ir a pescar, recién allí se puede brindar esa información públicamente. Si esta información sale antes podría generarse un conflicto. Bajo esas circunstancias, esta información es confidencial.
Por ello, entiendo que otros ministerios, como el de guerra o el poder judicial por ejemplo, que manejan casos muy sensibles, y que esa información salga sería crítico para el Estado pudiendo ser un problema crítico.

Yo: ¿Y qué factores cree que se vienen presentando para que esta norma no se implemente en las instituciones del Estado, habida cuenta de las diferentes normatividades que se han dado respecto de la seguridad de información?
E: Yo pienso que existen 03 factores:
El primer factor son los diferentes cambios que se dan en ONGEI. Hay muchos cambios de jefes, no duran mucho tiempo. Nosotros venimos implementando más bien por la presión de la Contraloría, ya que ellos son los que nos observan y empapelan. Por tanto, nosotros más estamos por la Contraloría que por la ONGEI.
El segundo factor se da en las entidades púbicas, donde también hay cambios de autoridades. Cambia el Ministro, cambia el Director Ejecutivo y entonces cambian las prioridades. Por ejemplo, el anterior Director no me daba prioridad para nada, el actual si da prioridad. Pero vamos a suponer que más adelante cambien a la Alta Dirección y por ahí me quitan el apoyo, y por ende el presupuesto que ahora me están dando.
El tercer factor es el recurso humano. Por ejemplo, se han hecho talleres de concienciación, donde a veces el usuario no tenía reparos en utilizar un USB sin medidas de seguridad y eso se les ha ido enseñando. Pero también en la parte técnica se adolece de medidas de seguridad de la información, hay programadores que no tienen en cuenta esto, jede de desarrollo que no ha leído la norma siquiera. Además,

no hay personal capacitado eficientemente en el Estado para implementar esta norma, la mayoría estamos en proceso de aprendizaje. En las reuniones de ONGEI cuando asistimos, la mayoría de los oficiales de seguridad que van allí están así, además que muchos recaen en el jefe de informática.
Un factor que además habría que agregar es el presupuestal, la cual está ligada a la politización de las Alta Dirección respecto del apoyo que le den a esta norma.

Yo: ¿Tiene conocimiento de alguna norma de seguridad anterior a la NTP 27001 actual?
E: Claro, estaba la NTP 17799, que estaba enfocada a los procedimientos y controles en sí, no a todo el sistema de gestión y allí implementamos ciertas políticas de seguridad de la información.

Yo: ¿Y sabe si alguna entidad del Estado implementó con éxito esa norma 17799?
E: Tengo entendido que la ONP, ONPE y RENIEC. Luego salió la norma 27001 y te cambia la figura ya que la anterior estaba orientada a la parte operativa y no a la gestión; cuando desde un inicio debió ser en la parte de gestión primero y luego en la parte operativa.
Pero tampoco era que se tenía que cambiar todo. Sino, tomar lo que se tenía, enmarcar en un enfoque más general y gestionarlo. No se perdía todo lo avanzado.

Yo: ¿Y para Ud. si compara la 27001 con la 17799, cuál de estas 02 normas fue más beneficiosa o más fácil de implementar?
E: Pienso que la norma 17799 tuvo más impacto que la 27001, porque podías mirar el procedimiento, atacabas algo puntual. Por ejemplo, en el caso de las políticas de resguardo o de backup de la información atacabas directamente esa política. Después, ejecutabas la política de control y mantenimiento de software. Es decir, ibas directamente a una política determinada.
Incluso esta norma, no se identificaba como activo sino como actividad o procedimiento. No estaba claro ese concepto, en cambio ahora si se maneja el concepto de "activo de la información".

Yo: Entonces, ¿Esas reuniones que hace la ONGEI si tienen algún impacto?
E: Claro que si tienen impacto. Ahí conversan los oficiales de seguridad, se dialoga e intercambian experiencias.

Yo: ¿Ud. cree que la ONGEI debe tener un rol más activo?
E: Si lo debe tener. Establecer una agenda de reuniones periódicas quincenal o mensual. Debe tener mayor liderazgo. Actualmente, cada institución del estado camina a su manera de la mejor forma que puede. Con ese liderazgo podríamos avanzar mucho más. Es un problema político.

Respecto de la <u>Parte Institucional</u>:

Yo: ¿Ud. tiene implementado actualmente la NTP 27001 en su Institución?
E: No. Estoy en proceso de implementación

Yo: ¿Qué beneficios cree Ud. que tendría en su Institución la implementación de la NTP 27001?
E: Si tendría beneficios en el sentido de la clasificación de la información que maneja la entidad, la cual antes no lo teníamos y que con la Ley de Transparencia muchas personas y entidades nos pedían todo tipo de información y que con el SGSI hemos podido ordenar y saber qué información brindar y cuál es confidencial. ,
Inclusive, el Director Ejecutivo tiene total conocimiento de ello y ahora se analiza la información a brindar y a quién. Todo pasa por el SGSI cuando alguien pide una información determinada. Se le consulta al oficial de seguridad de información antes de brindar cierta información solicitada, lo cual antes no pasaba, se entregada directamente. Por ello, si lo veo beneficioso.

Yo: ¿Existe el apoyo de la Alta Dirección en su Institución para la implementación de la NTP 27001?
E: El apoyo de la Alta Dirección es parcial, no es total. Por ejemplo, hubo un taller del SGSI con la Alta Dirección, la cual se tuvo que suspender porque no hubo suficientes asistentes. Entonces, tuvimos que conversar con el Director Ejecutivo para que él mismo coordine y asistieran los directores de las áreas a dicho taller. Es decir, que si el Director Ejecutivo no convoca a los Directores directamente, entonces no éstos no asisten o mandan a otro personal que no tiene poder decisorio en su área; incluso a veces envían a la secretaria administrativa a que asista o un practicante, es decir, por cumplir. Pero eso no es, la idea es que el jefe mismo se involucre, aporte y retransmita a todos sus subordinados

Yo: En esta Institución, el oficial de seguridad de información pertenece al área de informática, ¿Es asi?
E: Así es. El oficial de seguridad de la información también es de la oficina de informática. Y en este caso, soy yo.

Yo: Pero revisando en su organigrama, esta oficina de informática no es un área decisoria, es decir no depende directamente de la Alta Dirección, sino que depende de la Oficina de Administración.
E: Así es. En el año de 2012, con el cambio de gobierno, nos cambiaron toda la estructura porque antes la oficina de informática dependía directamente del Director Ejecutivo.

Yo: ¿Y esto influye en las decisiones de la implementación del SGSI?
E: En parte si y en parte no, porque al final nuestra función es transversal a todas las áreas de la institución. De repente, el camino formal es que se hace más lento. Porque por ejemplo, un informe antes se derivaba directamente al director ejecutivo, mientras que ahora tiene que ir a la OGA, de ahí pasa a la secretaría general y recién allí al director ejecutivo. Operativamente no tengo problemas en la implementación, el problema es la parte formal del asunto. Pero en general, si hay el apoyo de la Alta Dirección, y esto se refleja en el presupuesto asignado para la implementación del SGSI.

Yo: ¿En qué nivel o fase de la 27001 se encuentra su institución?
E: Estamos en la Fase III. Nosotros ya tenemos el oficial de seguridad de la información, tenemos un comité de trabajo y tenemos nuestro análisis de riesgo y estamos desplegando los controles. Ahora, la parte técnica la verá el oficial de

seguridad con un equipo de consultores dejando la parte administrativa al comité de trabajo de la institución.

Yo: ¿Quién lidera este comité de trabajo de seguridad de la información?
E: Ahí viene el problema, ya que es el oficial de seguridad es el lidera el comité de seguridad de la información. Pero con la nueva norma aprobada, donde dice que el que debe liderar el comité es el director ejecutivo o el que se designe en su representación.

Yo: ¿Cree Ud. que la Alta Dirección tiene claro lo que es el SGSI y qué importancia tiene?
E: No todos en la Alta Dirección lo tienen claro. Por ejemplo, algunos directores son biólogos, pero la mayoría sí. Justamente, y debido a esto, se ha separado un presupuesto para brindarles un curso de concienciación a todos los directores y allí explicarles bien la importancia.

Yo: ¿Está de acuerdo Ud. con que el área de informática sea el que lidere la implementación del SGSI?
E: No estoy de acuerdo porque, si bien el jefe de informática lo podría liderar, por su misma formación podría confundir lo que es seguridad informática con seguridad de información. Además, el oficial de seguridad debe depender directamente de la Alta Dirección porque él tiene un rol más amplio que el jefe de informática, uno es operativo pero el otro es el supervisor, el que hace el monitoreo respecto de si se cumplen las políticas y normas. Por tanto, en mi opinión el oficial de seguridad no debería ser el jefe de informática.
Un problema de esto es que no está normado el oficial de seguridad en el ROF y MOF del Estado Peruano. No es una obligación. Y mientras no esté oficializado así, no se va a poder avanzar mucho en este tema. La mayoría de las entidades contrata por CAS y estas personas se terminan yendo finalmente.
Estando en el ROF y MOF de la plaza va a tener que estar allí obligatoriamente. Este es un trabajo pendiente de ONGEI directamente y que además establezca que no dependa del área de informática sino de la Alta Dirección.

Yo: ¿Cuál es el Alcance del SGSI que Uds. vienen implementando en la institución?
E: El Alcance del SGSI que se ha definido implementar en la Institución es el Centro de Datos del área de informática. Esto se determinó luego de tener una reunión con todos los Directores para determinar un proceso de una dirección, pero un problema que tenemos es que los procesos no están debidamente formalizados. Acá los procesos técnicos que se manejan son muy científicos, muy biológicos, es un mundo bastante complicado. Entonces, definir un proceso core de la institución sería muy engorroso.
Además, la norma te dice que se puede elegir un proceso de negocio estratégico como hay también procesos que son críticos para la continuidad del negocio. Bajo ese enfoque, es que se decidió elegir el Data Center como Alcance del SGSI. Inclusive, tuve en una reunión en el MEF y allí también se viene implementando sobre el Centro de Datos. Ellos incluso querían implementarlo en la Dirección

General de Presupuesto Público, pero nuevamente allí también el problema era que no tenían claro los procesos que se manejan.

Es todo un tema el de los procesos, hay que mapearlos, definirlos, revisarlos y oficializarlos y eso genera todo un problema. Creo que los únicos procesos que están medianamente establecidos con directivas son los procesos administrativos, y hasta por allí nomas, ya que cada sector tiene su manera de trabajar.

Yo: ¿Y cree Ud. que si el oficial de seguridad no fuera de informática, también se hubiera decidido que el Alcance de implementación del SGSI de la Institución sería el data center?
E: Yo estoy más que seguro que si sería el Centro de Datos. Porque nosotros tenemos servicios informáticos que cruza información operativa de todas las áreas y todo eso está almacenado en el Data Center. Entonces en reunión del comité de trabajo de seguridad de la información se decidió definir al Data Center como el Alcance del SGSI en esta Institución. Allí también se dieron cuenta que los procesos técnicos no están definidos. Más bien, recién se está contratando una consultoría para realizar un mapa de procesos de la institución.

Yo: ¿Y se tienen bien definidos los procesos que intervienen en el data center?
E: Bueno, los procesos los tenemos mapeados con COBIT5 pero asimismo no los tenemos formalizados.

Yo: ¿Y este Alcance del SGSI ya se encuentra documentado?
E: Claro, el Alcance del SGSI en la Institución ya se tiene documentado y solo está para aprobarse. La empresa que se contrató lo elaboró según nuestras especificaciones y nos entregaron el Alcance y las políticas de seguridad ya definidas.

Yo: Entonces se puede decir que el oficial de seguridad de la institución monitorea el trabajo que viene realizando la empresa consultora respecto del SGSI?
E: Así es. Es por un tema de tiempo y ocupaciones. Entonces, la empresa ya me proporcionaron sus entregables y esto va a pasar al comité de seguridad para su revisión y elevado posteriormente a la Alta Dirección para que, mediante una Resolución, se publique oficialmente en la entidad.

Yo: ¿La estructura organizacional actual de la institución favorece o restringe el desarrollo del SGSI?
E: Lo restringe bastante. Primeramente, porque antes ésta área tenía más peso. Ahora todo debe coordinarse antes con administración y no es una coordinación directa con la Alta Dirección. Se tenía un rango más alto.

Yo: En el caso de la metodología de riesgos, ¿qué metodología están aplicando?
E: Es una metodología propia. La empresa consultora ha aplicado una metodología de riesgos propia que sigue los lineamientos de la norma, los cuales son:
la identificación de riesgos, la evaluación de riesgos y termina con el tratamiento de los riesgos. Partiendo todo de la identificación de los activos.

Yo: ¿Y cómo percibe Ud. la cultura organizacional de la Seguridad de Información en la institución?
E: Digamos que es el comité de seguridad de la información que son los que difunden el SGSI al personal que trabaja con ellos y que ya en parte han tomado conocimiento y concientización sobre ello. Aunque aún hay usuarios reacios que no entienden de no traer un USB por ejemplo.
Incluso ha habido 04 charlas de concientización en seguridad de la información, por parte de la empresa consultora, para todo el personal de la institución, pero no es suficiente aún. Igualmente, ya estamos en ese camino. Además estamos implementando un intranet donde se van a colocar todas las políticas de seguridad de la información para el personal.

Yo: ¿Qué piensa de la actualización de la norma NTP 27001:2014 respecto del enfoque que le están dando?
E: Me parece que está bien, porque le asignan responsabilidad al director ejecutivo; lo que antes no tenía. Me parece interesante porque ahora si le están dando el debido peso que se debió dar desde un inicio.

Yo: ¿Cómo se ha realizado la capacitación de la implementación del SGSI en la institución?
E: Bueno, se han dado 02 tipos de capacitación: Talleres de concienciación enfocada al comité de seguridad de la información y talleres de concienciación para el personal de la institución. Pero esto ha sido desde al año pasado por que nos asignaron presupuesto para este proyecto del SGSI.

Yo: ¿Y antes del año pasado, cómo se manejaba este tema de la capacitación de la implementación del SGSI en la institución?
E: Nada, no se hacía nada. Porque no había presupuesto para ello, ni por terceros ni por otro lado. A pesar de que lo solicitaba con documento, no me lo pasaban porque no tenía partida presupuestal para ello. Pero ahora, contamos con presupuesto para este proyecto y se pueden ejecutar acciones que conlleven a su implementación.

Yo: ¿Qué otros factores más cree Ud. que influyen en la implementación del SGSI en su institución?
E: Un factor crítico y clave es el ROF y MOF en todas las entidades públicas por parte del gobierno central. Porque es ahí donde tiene que ubicarse al oficial de seguridad y que tenga presupuesto perenne. Actualmente, así como está, el oficial de seguridad no existe en el mapa estatal.
Estando en el ROF y MOF, va a ser como un área que ya existe en el organigrama de la institución con su propio presupuesto. Incluso se va a tener una responsabilidad funcional como oficial de seguridad en el Estado.

Yo: ¿Algo más que quiera agregar al respecto?
E: Me parece que sería bueno reunirnos un grupo de entidades para intercambiar ideas y experiencias en el avance de la implementación del SGSI en las instituciones públicas. A veces nos falta un poco más de unión como Estado, cada entidad como que trabaja en lo suyo, no se comparten aprendizajes. Se podrían hacer convenios interinstitucionales porque la ley me permite hacerlo incluso.

ANEXO 11: TRANSCRIPCION DE LA 4ta. ENTREVISTA

La entrevista está dividida en 03 partes:

La primera tiene que ver con la parte más técnica, es decir con la experiencia laboral y personal que Ud. tenga con respecto a la seguridad de información. Una segunda parte normativa, que son preguntas referidas a la misma norma y con la ONGEI misma que es el ente que norma este proyecto. Y una tercera parte operativa, que son preguntas del SGSI en su Institución, es aquí donde desarrollaremos más profundamente el tema de la tesis de investigación

Entonces, respecto de la Dimensión Técnica:

Yo: ¿Cómo define Ud. lo que es un Sistema de Gestión de Seguridad de Información?
E: Es el armado de un conjunto de componentes de manera localizada que te permiten cuidar y garantizar la confidencialidad, integridad y disponibilidad de la información dentro de una institución.

Yo: ¿Qué experiencia profesional tiene Ud. respecto de la Seguridad de Información?
E: Bueno, he participado en varias implementaciones del Sistema de Gestión de Seguridad de la Información ya certificados como ONP, RENIEC y ONPE

Yo: ¿Ud. pertenece o ha pertenecido a alguna asociación vinculada a la Seguridad de Información?
E: Si, pertenezco a ISACA (*). Tengo 03 certificaciones de ISACA: CISA, CISM y CRISK.

Respecto a la Dimensión del Proyecto, es decir preguntas técnicas referidas a la norma técnica 27001:

Yo: ¿Para Ud. qué es la NTP 27001 y qué papel cumple la ONGEI en la implementación de esta norma?
E: La NTP 27001 es la traducción del estándar internacional de seguridad de la información y es aquí donde se establecen los requisitos y controles que son un conjunto de buenas prácticas para poder gestionar la seguridad de la información en una institución.

Respecto de la ONGEI puedo decir que es el organismo rector o director en lo que se refiere a gobierno electrónico y dentro de esas funciones está también normar la parte de seguridad de la información.

Yo: ¿Qué objetivos cree Ud. que busca el Estado Peruano con la implementación de la NTP 27001?
E: Bueno, mejorar la seguridad de la información de las instituciones a través de la implementación de prácticas internacionales. Todo va alineado al Plan Bicentenario, ya que si nosotros como país estamos yendo hacia un gobierno electrónico, de todas maneras tenemos que reforzar la parte de la seguridad de la información y ahí es donde entra la ONGEI, ya que la seguridad de la información es un componente importante para el desarrollo del gobierno electrónico.

Yo: ¿Qué factores cree Ud. que vienen influyendo en la implementación de esta norma en el Estado Peruano?
E: Primeramente, el incremento en el uso de la tecnología de información en el Perú y el mundo, donde al haber mayor tecnología hay mayores riesgos y al haber mayores riesgos hay mayor necesidad de seguridad de la información, eso es algo que promueve que las empresas estén enfocándose en la seguridad. Inclusive los organismos reguladores también están enfatizando más esta parte, haciendo auditorías y revisiones en lo que respecta a seguridad de la información.

Yo: ¿Cree que se viene implementando bien o no el SGSI en el Estado Peruano?
E: Pienso que como Estado no trabajamos en equipo, ya que siendo instituciones públicas regidas a través de ONGEI todavía no llegamos a ese punto de trabajar como gobierno. Veo esfuerzos aislados de algunas instituciones, pero no veo un esfuerzo orientado hacia una implementación en conjunto.

Actualmente, cada entidad tiene que contratar sus propios asesores y su propio personal para poder realizar esta implementación. Cuando me parece que esto debía realizarse Si no se puede manejar esto a nivel de sectores porque tienen muchas instituciones, por lo menos a través de sectores de gobierno. Por ejemplo, en el Ministerio de la Mujer hay varias organizaciones y todas trabajan por su cuenta, donde si cada aportara su experiencia en seguridad sería mucho mejor. Otro ejemplo vendría a ser el de SUNAT, donde tienen implementada la parte de seguridad de la información mucho más desarrollada que otras entidades; Entonces, si ellos pudieran enseñar a otras entidades que son más pequeñas y que no han requerido hasta ahora de tanta seguridad de la información, esto podría salir mucho rápido, podría aminorar costos. Todo esto debería articularse a través de la ONGEI.

Yo: ¿Cree entonces que la ONGEI viene cumpliendo su papel de ente rector?
E: Pienso que la ONGEI viene cumpliendo un papel de ente normativo, pero no está haciendo un papel de ente implementador, tampoco no se difunde mucho cuál es el tipo de ayuda que te puede dar la ONGEI. Por ejemplo, un amigo que trabaja en un Ministerio, tuvo un problema de ataque de negación de servicios, y en este caso la ONGEI tuvo un rol muy activo en esto. Ellos fueron a la institución y lo ayudaron a armar su plan de contingencia, inclusive le instalaron herramientas para monitorear, todo esto por la ONGEI a través del PeCERT. Yo no sabía que este tipo de cosas lo podíamos solicitar al PeCERT.

Entonces, este tipo de cosas debería replicarse en el SGSI. Por ejemplo, nosotros sabemos que todas las instituciones requieren de un servicio de Ethical Hacking, y en el caso anterior que te comenté, el PeCERT le hizo un análisis de vulnerabilidades, que si bien era pequeño pero hasta eso le hicieron. Por lo tanto, si el Estado pudiera formar personas que pudieran hacer este tipo de labor de repente funcionaría la implementación o al menos asesoraría en la implementación del SGSI en el Estado, porque muchas instituciones a veces por desconocimiento terminan haciendo TdR de implementaciones de servicios de seguridad de información que en realidad no son las más óptimas, ya que muchas veces se dejan orientar por un mal

proveedor y terminan haciendo términos de referencia que no benefician a la institución sino únicamente al proveedor.

Yo: ¿Cree Ud. que normas técnicas anteriores a la 27001 han sido más beneficiosas o menos que la norma actual?
E: Bueno, primeramente yo entré al mundo de seguridad de la información con la 27001, por lo que no podría decirte si fue más o menos beneficiosa.

Yo: Hace poco se ha aprobado la NTP 27001:2014 ¿Cree Ud. que esto va a beneficiar más o no a la implementación actual en las Instituciones del Estado?
E: Para mi va a ser lo mismo porque si bien esta NTP 27001:2014 en estructura es más ordenada que la anterior, pienso que el beneficio de la implementación del SGSI no va a depender de esta norma, porque solo es una traducción del estándar. De todas maneras van a haber entidades que van a implementar mejor pero eso no es consecuencia de esta nueva norma sino es consecuencia de la evolución en seguridad que van adquiriendo las instituciones.

Respecto a la Dimensión Institucional, es decir preguntas referidas a la seguridad de la información en su institución:

Yo: ¿Cómo cree Ud. que viene beneficiando en su institución la implementación de la Norma Técnica 27001?
E: Bueno, la NTP 27001 en mi institución se aplica la seguridad de la información de manera muy fuerte debido al tipo de trabajo que realizamos como son los procesos electorales. Por tanto, la implementación de la seguridad de información viene desarrollándose hace muchos años y lo que se hace es mantener ordenada la implementación de controles de seguridad, muchos de los cuales ya estaban creados hace años. Entonces, lo que se viene haciendo es establecerlos y mejorarlos a través de un sistema de gestión.

Yo: ¿Osea que les ha ordenado la forma de trabajarlos?
E: Bueno, lo que nos ha ordenado también la forma de trabajar es que nosotros no sólo tenemos ISO 27000, nosotros también tenemos ISO 9000. Entonces, el conjunto de estos ISO´s (27000 y 9000) ha hecho que los procesos estén más ordenados.

Yo: Justamente ¿Uds. primero se han certificado en ISO 9001, y después esos mismos procesos los han llevado a la 27001? ¿Es así?
E: Estamos en eso. Porque no es la intención en este momento pasar todos los procesos. Actualmente, nosotros tenemos certificados 11 procesos (en 9001), y de estos no todos van a tener 27001 sino solamente aquellos en los que se requieran niveles de seguridad.

Yo: Entonces, ¿Se puede decir que Uds. para iniciar la implementación de la 27001 tomaron este esquema de trabajo?
E: Si, así es.

Yo: ¿Sería aconsejable implementarlo de esa forma para otras Instituciones?
E: Bueno, a mi parecer el ISO 9000 te da un buen soporte, porque para implementar ISO 27001 necesitas tener los procesos bien definidos y claros. Y muchas veces esto

no lo ves tan claramente si vas directo a la 27001. Ahora, lo que también se puede hacer es implementarlos (ISO 9001 é ISO 27001) en paralelo.
Nosotros lo que hemos optado por hacer es que los procesos que requieren seguridad de la información y que ya tienen ISO 9001, son los candidatos a pasar a 27001. Primero porque es más fácil, ya tienes una infraestructura de sistema de gestión y sobre eso implementas controles y todo lo que es gestión de riesgos.
Por ejemplo, la institución en aquellos documentos normativos que son base de un sistema de gestión como son las auditorías internas, acciones preventivas, correctivas o control de registros, ya esa parte la tenemos acotada dentro de un sistema ISO 9000.

Yo: ¿Ud. cree que es importante tener los procesos claros antes de implementar seguridad de información?
E: Si es importante, porque si no tienes los procesos claros al momento de identificar los activos de información, si tú no tienes bien definido un proceso primeramente no puedes planificar bien tu Alcance del SGSI y, por tanto, durante a identificación de los activos pueden pasarse algunos que son importantes y que puedes no haberlos identificado. En cambio, tener un proceso claro te da una visión de negocio y con eso puedes identificar bien lo que quieres implementar.

Yo: Tengo entendido que a partir del ISO 9001 se creó un área de Gestión de la Calidad y que es la que ve los procesos ¿Es así?
E: Si. Es una gerencia que da las pautas en lo que es gestión por procesos y que también ve todo el tema de las certificaciones 9001 y 27001.

Yo: ¿Existe el apoyo y la claridad necesaria de la Alta Dirección para la implementación del SGSI en su Institución?
E: Si existe. Tiene clara la importancia de la implementación del SGSI y está dentro de sus objetivos y, a diferencia de otras instituciones, el jefe nacional es un "fanático" de los sistemas de gestión, inclusive es auditor líder en 9001.

Yo: ¿Si en su Institución cambiaran de personal de Alta Dirección, habría una continuidad de la documentación en la implementación del SGSI?
E: Claro, porque justamente un sistema de gestión lo que te da es eso. Te provee de toda la documentación para tener esa continuidad, te marca la línea.

Yo: ¿El Oficial de Seguridad de la Información pertenece al área de TI?
E: No, no pertenece a TI. El oficial de seguridad pertenece a la gerencia de gestión de la calidad.

Yo: Siendo su institución una entidad a nivel nacional, ¿Cómo hacen Uds. para llevar implementar la Seguridad de la Información en las distintas regiones del país?
E: A ver, por ahora las políticas de seguridad de la información se replican a nivel nacional en un proceso electoral, pero todavía el Alcance del SGSI como tal no está implementado a nivel nacional.

Yo: ¿Entonces quién lleva el control en las distintas regiones?
E: Lo que pasa es que en el caso de las regiones esta institución es muy chica cuando no hay procesos, en cambio cuando si hay procesos es bien grande y se contrata una gran cantidad de personal. Cada oficina tiene un responsable (un jefe de ODPE y un

encargado de cómputo), el cual tiene la responsabilidad de cuidar la seguridad de la información dentro de su ámbito.

Yo: ¿Dentro de la organización del SGSI, tienen un comité técnico y un comité de gestión tal como lo recomienda ONGEI?
E: Bueno, tenemos a la Alta Dirección a la cabeza y un Comité de Gestión de Seguridad de la Información cumpliendo las funciones respectivas de seguridad. Dicho comité está conformado por casi todos los gerentes; y de ahí hay un Comité Operativo, que está conformado por los responsables de Seguridad de la Información de cada gerencia.

Yo: ¿Y en esas reuniones del comité de gestión de seguridad de la información, van realmente los gerentes o mandan a otra persona?
E: No, casi todos van. Muy en parte porque el jefe nacional es promotor de este tipo de sistemas de gestión, y esto hace que todos los gerentes estén alineados a esto. Este comité se reúne 3 a 4 veces al año máximo, pero para eso tienes a los comités operativos.

Yo: ¿Cómo están conformados estos comités operativos de seguridad de la información?
E: El comité operativo está conformado por los responsables de seguridad de cada gerencia, los cuales no son gerentes sino especialistas, no en seguridad sino en las funciones de su gerencia; por ejemplo, un abogado especialista en temas informático-legales. Y allí, el Oficial de Seguridad trabaja con estos especialistas.

Yo: Cuándo se define el Alcance de Seguridad de la Información o los documentos del SGSI, ¿Quién los elabora o desarrolla, el comité operativo?
E: A ver te explico, si los documentos son netamente técnicos entonces los elabora la gerencia de informática y luego lo revisamos nosotros como área de seguridad, o sea la gerencia de calidad. Después de ello, es convocado el comité operativo de seguridad para poder validar toda esta propuesta. Una vez que está validada por todos los responsables, ésta se eleva al comité de gestión de seguridad que lo revisa y aprueba la propuesta, y lo presenta a la jefatura nacional para su aprobación.

Yo: Es decir que la elaboración de la documentación del SGSI, ¿Siempre interviene el área de Tecnología de la Información?
E: Si, también interviene TI. Partimos de un concepto: Si bien la gerencia de TI o alguna otra gerencia puede crear un documento de seguridad, trabajamos siempre en equipo, en donde las políticas de seguridad te las da la gerencia de calidad porque ahí está el oficial de seguridad y el área de seguridad también. Pero si es importante trabajar con las demás áreas, porque ellos tienen que saber lo que se está creando, las políticas que se están dando. Si no fuera así, después va a ser mucho más difícil que estas áreas quieran implementarlo o hacerlo. Por ejemplo, para nosotros es muy importante la opinión legal, así como también es importante la opinión de cada una de las áreas operativas.

Yo: ¿Cómo realizan la consulta para intercambiar opiniones, se les reúne a todos o cómo se les consulta a cada uno?
E: Primeramente, es muy importante la opinión de cada una de las áreas operativas. Para ello, se les envía la propuesta que se tiene en un correo electrónico para su

revisión. De esta forma, cada uno de los integrantes puede ver la factibilidad de la implementación de todos los controles y también tenemos la oportunidad de justificar por qué debemos utilizar un control y es más fácil de que eso se pueda implementar.

Yo: ¿Osea que hay bastante comunicación entre el Oficial de Seguridad y el Comité Operativo?
E: Claro. El Oficial de Seguridad es el presidente del Comité Operativo y es el que lleva la propuesta al Comité de Gestión.

Yo: ¿A su parecer, la estructura organizacional actual en su institución favorece o restringe el desarrollo del SGSI?
E: Bueno, hasta ahora ha favorecido pero puede mejorar. Por ejemplo, si bien tenemos un área a cargo de la seguridad de la información dentro de la gerencia general, pero a nivel del ROF y MOF no existe un área de seguridad.

Pienso que esto es parte de la maduración que vamos teniendo, ya que si bien actualmente tenemos un proceso certificado en 27001, la proyección es llegar a 5 procesos certificados.

Yo: Ud. me ha referido que actualmente el Oficial de Seguridad de su institución está ubicado en la gerencia de gestión de la calidad, ¿Pero antes de eso donde estaba este oficial?
E: El Oficial de Seguridad estaba en Secretaría General. Cuando hace menos de un año se crea la gerencia de Gestión de la Calidad, el Oficial de Seguridad pasa allí, pero nunca ha estado en TI. Aunque si tengo entendido que mucho antes de todo esto, se designaba a una persona de TI con las funciones de Oficial de Seguridad pero que no era a tiempo completo como sí lo es ahora.

Yo: ¿Puede ser que las Instituciones del Estado no tengan bien claro en qué área debe estar el Oficial de Seguridad?
E: Yo creo que la mayoría de las instituciones confunden o limitan la seguridad de la información solamente al área tecnológica y eso es un error, porque dejas de lado todas las demás áreas y las demás personas no se quieren involucrar mucho porque piensan que eso una tarea de TI.

Yo: ¿Cómo percibe Ud. la cultura organizacional del SGSI en su institución?
E: Dentro de los Comités ya tienen bien definido cuál es su rol y qué es lo que tienen que hacer porque ya vienen trabajando con este esquema.

Dentro del personal de la institución aún falta. Sin embargo, la seguridad de la información es un componente dentro del programa de inducción. Después en las áreas operativas, cuando hay cambios de puestos o de nuevo personal, éstas pueden solicitar capacitación en seguridad de información.

Yo: ¿Y hay algunas formas de difundir el SGSI a nivel interno y externo de la institución?
E: Bueno, utilizamos enviar información por mail y así también tenemos una intranet donde están las políticas de seguridad de la información publicadas.

Yo: ¿Qué metodologías de gestión de riesgos utilizan en el SGSI?
E: Bueno, utilizamos una metodología propia pero hasta hace unos meses veníamos trabajando con una adaptación de la metodología ISO 27005 pero ahora lo que hemos hecho es irnos hacia la ISO 31000.

Yo: Si Uds. ya vienen implementando el SGSI, ¿Qué problemas han surgido que hayan tenido con seguridad de la información?
E: Bueno, problemas fuertes de implementación no hemos tenido. El mayor obstáculo que se presenta siempre es la de crear conciencia al personal, es cambiar los hábitos y eso es bien difícil para modificarlos en las personas. Ese sería el principal inconveniente que tendríamos. Pero siempre estamos aplicando algunas estrategias para cambiar esto.

Yo: ¿Qué otros factores cree Ud. podrían estar impidiendo o afectando en la implementación del SGSI en las Instituciones del Estado?
E: Bueno, uno de los factores es pensar que seguridad de la información está asociado netamente a informática, que es una función de TI. Otro factor es la falta de conocimiento o de importancia que le de Alta Dirección al tema de seguridad de la información y pienso que es un factor muy importante el poder vender la seguridad de la información en las instituciones. Me parece que este debería ser un trabajo a nivel de ONGEI. Así como ONGEI reúne a los Oficiales de Seguridad, podría reunir a todas las altas autoridades del Estado y brindarles una capacitación en SGSI. Tengamos en cuenta que la NTP 27001 es una Política de Estado.

Por ejemplo, así como tenemos una Política Nacional de Calidad podríamos tener una Política Nacional de Seguridad de la Información, pero más que dar la norma deberíamos buscar la forma de todos conozcan la importancia de la seguridad de la información en cada una de sus instituciones. De repente una persona de TI, por más que quiera, no tiene de repente la capacidad como para poder transmitir esto a la Alta Dirección, ya que tienes que ver cómo vas a expresar riegos y seguridad pero tienes que expresarlo en términos que te pueda entender la Dirección, y muchas veces el oficial de seguridad o quien asuma esta función no conoce mucho del negocio.

Yo: ¿Existe suficiente personal con experiencia en la implementación del SGSI en el Perú?
E: Si hay personal con experiencia en seguridad de la información pero no como para atender a todas las instituciones del Estado, porque muchas de ellas están avocadas al tema de banca.

ANEXO 12: TRANSCRIPCION DE LA 5ta. ENTREVISTA

La entrevista está dividida en 03 partes:

La primera tiene que ver con la parte más técnica, es decir con la experiencia laboral y personal que Ud. tenga con respecto a la seguridad de información. Una segunda parte normativa, que son preguntas referidas a la misma norma y con la ONGEI misma que es el ente que norma este proyecto. Y una tercera parte operativa, que son preguntas del SGSI en su Institución, es aquí donde desarrollaremos más profundamente el tema de la tesis de investigación

Respecto de la Dimensión Técnica:

Yo: ¿Cómo define Ud. lo que es un Sistema de Gestión de Seguridad de Información?
E: Bueno un sistema de gestión de seguridad de información es un conjunto de directivas, normas, procedimientos y estructuras organizativas funcionales y legales que van a garantizar la confiabilidad, integridad y disponibilidad de la información.

Yo: Respecto de su experiencia personal y profesional respecto de la seguridad de información ¿Nos podría hablar un poco?
E: A ver. Yo me he desempeñado 06 años como auditora de sistemas, tanto en órganos de auditoría privados como gubernamentales en el Ministerio del Interior, la Municipalidad de Lima y SUNASS. Luego me estoy desempeñando ya en el campo de seguridad de la información desde junio del 2012 hasta la actualidad

Yo: ¿Ud. pertenece o ha pertenecido a alguna asociación vinculada a la seguridad de información?
E: Si, soy miembro de ISACA la cual es una institución internacional de lo que es auditoría y seguridad de la información. Además, esta organización brinda unos certificados que validan la profesionalización en estos campos. En ese aspecto tengo 02 certificaciones: CISA (certificación como auditor de sistemas de información) y CISM (certificación como gestor o gerente de seguridad de la información).

Respecto a la Dimensión del Proyecto, es decir preguntas técnicas referidas a la norma técnica 27001:

Yo: ¿Para Ud. qué es la Norma Técnica Peruana 27001 y qué papel cumple la ONGEI en la implementación de esta norma?
E: Bueno, la NTP 27001 es una norma que está homologada con la ISO 27001 y la ONGEI es el órgano rector autorizado para emitir las directivas y normativas que van a regir en las instituciones del Estado en cuanto a los temas de informática.

La norma de seguridad 27001 no es una norma que está únicamente centrada en informática, pero dado el desconocimiento y a falta de concienciación que genera, se le asocia mucho a lo que es TI y fue la ONGEI quién tomó la iniciativa de formalizar esta norma. Por eso es que ONGEI la propuso, pero en realidad la ha aprobado la Presidencia del Consejo de Ministros (PCM).

Yo: ¿Qué objetivos cree que busca el Estado Peruano con la implementación de esta norma?
E: En la actualidad, el activo más importante de una entidad pública o privada es la información. Como activo primordial merece ser resguardado, cuidado y protegido. Por eso es que el Estado ha tomado cartas en el asunto y está buscando proteger su activo más importante y ha sacado esta NTP. De allí la importancia de implementarlo a nivel de Estado. La NTP 27001 es de obligatoriedad para las Instituciones del Estado, mientras que para la empresa privada es potestativo.

Yo: ¿Qué factores cree Ud. que vienen influyendo en el Estado en la implementación de la NTP 27001?
E: El factor más importante para que no se haya podido implementar hasta ahora en el Estado es la falta de conciencia, la cual es incluso a nivel mundial; porque es un aspecto individual que se va replicando a nivel de masas. Todavía estamos tomando conciencia lentamente de la importancia de la seguridad de la información.

Lo vemos, por ejemplo en el facebook, cuando compartimos muy fácilmente a nivel individual nuestros datos. Es decir, no tenemos conciencia de cuán importante es lo que estamos publicando y cuáles son los riesgos a los que estamos expuestos. Si a nivel individual no tenemos conciencia de esa seguridad, a nivel institucional mucho menos.

Entonces, hacer que el área de TI que es un área de apoyo en todas partes, haga tomar conciencia a la Alta Dirección de lo importante que es la información es difícil. Y sobre eso, generar conciencia en cada uno de los individuos que conforman estas entidades es aún una tarea más titánica, tomando en consideración que las instituciones estatales son grandes. Por ejemplo, el Ministerio Público es gigantesco y hacerle tomar conciencia a cada uno de los trabajadores, que son 16,000, es muy complicado y requiere de muchos recursos; y a todo el Estado es muchísimo más difícil.

Ahora, esta tarea yo la veo con buenos ojos porque hemos empezado, se está haciendo. Yo no considero que nos falta ya que estamos en muy buen camino, porque lo importantes es haber empezado, se están tomando iniciativas desde ONGEI por ejemplo con la publicación de la norma. Se congrega a los oficiales de seguridad periódicamente, aunque lo ideal sería que capaciten y certifiquen a todo el mundo pero hay que ser realistas. Hay que tomar la parte positiva, están convocando, están incentivando a través de legislaciones, a través de información a que se concientice la seguridad. Además, hay una iniciativa de la ONGEI que se llama PeCERT que busca dar apoyo a las entidades del Estado en cuanto a incidentes de seguridad. No estamos en la panacea pero estamos caminando con lo pocos recursos que hay, porque esta falta de conciencia hace que las instituciones públicas no dispongan recursos económicos para la implementación de la seguridad de la información en sus instituciones.

Entonces la pregunta a hacerse es: "¿Cómo se puede lograr un cambio de conciencia si no hay recursos?". Porque lamentablemente se requieren recursos económicos para la difusión, para la implementación tecnológica; y todo eso implica recursos. Y para que la Alta Dirección de una institución pida presupuesto adicional tiene

primero que comprarse la idea de que la seguridad de la información es importante. Todavía no estamos maduros en el nivel de que digan: "Si, uno de los puntos principales es la seguridad".

Actualmente, las instituciones públicas están abordando el tema de la seguridad de la información por el lado de que no me hackeen mi página web, y eso es la mínima parte, digamos que el impacto es más que nada en la imagen. Pero hay otros impactos más fuertes que como no se ven, no se valorizan. Por ejemplo, si están robando información a través de la red de internet de una institución pública, eso no se puede ver; y como no se puede ver, no se puede medir el impacto; y por lo tanto no se toma conciencia.

Yo: ¿Tiene Ud. conocimiento de normas anteriores a la NTP 27001?
E: La norma 17799 fue la primera iniciativa de seguridad de información que sacó el Estado. Esta norma fue potestativa. Digamos que se recomendaba a las instituciones públicas que implementen las medidas según sus posibilidades y los controles que pudieran. Y como fue potestativo, nadie lo hizo. Ya con la norma 27001, se obligó a que todas la implementen. La dificultad aquí radica en que se da la norma pero hacen falta las herramientas y en eso está trabajando ONGEI.

Yo: Hace poco se ha aprobado la nueva norma NTP 27001:2014. ¿Ud. cree que esto beneficiará o no a su implementación?
E: La beneficia en el sentido de que es menos rígida, da más apertura a que las instituciones implementen según lo que tienen, según lo que saben, según lo que les ha funcionado. No los encasilla digamos a un solo método. Por ese lado, facilita pero otra vez regresamos a lo mismo: Si no hay decisión política institucional, por muy fácil que sea no se va a hacer.

Yo: Tengo entendido que algunas instituciones ya se han certificado, ¿Tiene conocimiento de esto o porque algunas lo han hecho y otras no?
E: El punto de partida primordial para implementar un SGSI es el respaldo de la Alta Dirección. Las instituciones que han certificado, y que son 4, lo que han tenido es eso. Han tenido el apoyo y el sponsor de la Alta Dirección.

La Alta Dirección dijo: "Es importante la seguridad de la información; Y por lo tanto, vamos a invertir en la certificación". Ellos han dispuesto un presupuesto para la implementación, porque no ha sido fácil, ha sido un desembolso de tiempo, de recursos, de dinero, de profesionales. No ha sido un mes, sino que han sido como 3 años por ejemplo que le ha tomado a la ONP implementar y certificarse sobretodo. Pero ha sido todo parte de la decisión política.

Se pueden tener los mejores profesionales, la gente de mando medio puede tener la mejor disposición pero si el respaldo no viene de la Alta Dirección, no va a tener llegada.

Respecto a la Dimensión Institucional, es decir preguntas referidas a la seguridad de la información en su institución:

Yo: ¿Cómo cree Ud. que viene beneficiando en su institución la implementación de la Norma Técnica 27001?
E: En mi institución, uno de los factores críticos es la información, sobretodo porque es información sensible de los ciudadanos. Ayudaría mucho que los litigantes, las personas que recurren a la institución tuvieran la certeza y la seguridad de la fiabilidad de su información; además, de poder acceder a ella de forma segura.

Yo: Si el Estado está solicitando que se implemente la NTP 27001 ¿Qué efectos cree Ud. que se lograrían en las instituciones públicas?
E: Para mi institución, así como para las demás entidades de administración de justicia, tienen un escollo o una deuda con la ciudadanía. La confianza en las instituciones se está perdiendo.

Y si a eso se le va a agregar la debilidad en cuanto a la confiabilidad y confidencialidad de la información, digamos que la confianza del ciudadano en las instituciones se va a deteriorar más. El hecho de que tengamos un sistema de gestión de seguridad de la información sostenible y robusta fortalecería esa confianza. En eso básicamente beneficiaría a la ciudadanía.

Yo: ¿En su institución existe el apoyo de la Alta Dirección para la implementación de la NTP 27001?
E: Sí, el apoyo está. Lo que falta es, talvez, un poco más de interiorizar la necesidad de esto. Porque tenemos una estructura organizacional que se ha generado para la seguridad de información (a través de un comité).

Digo que falta la interiorización porque aún no se le da la fuerza de otorgar recursos para ello. Aun no hay la asociación de importancia vs costo. La Alta Dirección sabe que es importante, saben todo el impacto pero todavía no lo asocian al desembolso de recursos.

Yo: ¿Qué estructura organizacional tienen instalada en su institución respecto del SGSI?
E: En mi institución se ha empezado por la contratación del oficial de seguridad (que soy yo), luego hemos formado el comité de seguridad de la información en la Alta Dirección. Con este comité se han empezado a establecer las directivas que luego son aprobadas por la gerencia general.

Se han tomado ya varias medidas. Por ejemplo: se ha implementado la firma del acta de confidencialidad, tanto para los trabajadores, para los terceros y para todas las empresas que entran. Cualquier persona que brinde algún servicio, algún contacto con la institución que no pertenezca a ella. Entonces, además del contrato hay una firma de confidencialidad. Esto para mí es un logro, porque ha costado mucho trabajo a los directivos y a las personas lo importante que es. Que en buena cuenta es una protección para ellos y es una protección para la institución.

Yo: La ONGEI recomienda tener un comité técnico y un comité de gestión, ¿Uds. también cuentan con esta estructura de comités?

E: Nosotros contamos con un comité de seguridad de información de Alta Gerencia que está formalizado. Por la naturaleza de la institución, nosotros contamos con una parte administrativa y una parte jurídica.

Pero, implementar directamente un SGSI en la parte jurídica iba a ser más complicado; aun cuando la teoría indica que tendría que hacerse en un área core del negocio, pero dada la naturaleza de la institución implementar un SGSI directamente en el core del negocio de esta institución que es tan grande y tan compleja, pudiera haber resultado en un fracaso. Por tanto, la estrategia que se trazó fue implementar el SGSI como piloto en un área en la que podamos implementar normas y directivas y donde podamos hacer el ensayo-error y tomamos por eso el área de TI.

Por eso, nuestra área piloto es TI, no hemos tomado un proceso sino un área. Es decir, tomamos todos los procesos de la gerencia de TI y allí también surgió otra dificultad de las instituciones públicas: ¿Por qué no podíamos agarrar un proceso? Porque las instituciones públicas no están organizadas por procesos, son organizaciones funcionales. Así que orientar el SGSI a un proceso es complicado. Además que, generalmente, sus MAPROs están desactualizados.

Todo esto es un tema muy complicado porque la norma (NTP 27001) establece, como punto de partida, que la institución funcione por procesos. Es decir que se asume que la organización funcione por procesos. El problema está en que nuestras organizaciones no funcionan por procesos, sino por funciones. Así que habría que adecuar la norma al funcionamiento de nuestras organizaciones. Allí se requiere mucho de pericia y sobretodo del apoyo de la gerencia donde se está implementando.

Yo: Sin embargo ONGEI recomienda realizar una implementación por procesos ¿Es así?
E: Claro, lo ideal es hacer la implementación por procesos pero yo creo que las únicas instituciones públicas que funcionan por procesos son las que están certificadas, y aun así yo no podría asegurarlo.

La institución donde laboro tiene como 30 años, es una organización muy grande. Entonces, convertirla a procesos es un proceso -valga la redundancia- muchísimo más amplio. Como hay que implementar la norma, más que por cumplir la norma, por asegurar el activo, hay que empezar con lo que hay, como está.

Yo: Y Uds., en su alcance, implementaron los procesos del área de TI, verdad?
E: Se implementaron controles en el área de TI, tratando de adecuar la norma a la forma cómo está estructurada el área de TI.

Yo: ¿Y en qué nivel o fase de la implementación incremental se encuentran?
E: Nos encontramos en la Gestión de Riesgos. Deberíamos haber avanzado más pero como no hay presupuesto, no hay personal.

Yo: ¿Existe presupuesto para la implementación del SGSI en su institución?
E: No existe presupuesto para seguridad de la información. El único presupuesto designado a seguridad son los honorarios del Oficial de Seguridad. Y, por lo tanto, no hay presupuesto para consultorías, para personas adicionales a seguridad.

Por ello, las tareas han tenido que ir avanzando poco a poco con el tiempo que les quedaba a otras personas para que apoyen al oficial de seguridad.

Yo: Entonces, uno de los principales problemas en las instituciones sería el presupuestal también ¿Es así?
E: ¿Podrían las instituciones públicas podrían prescindir de los sueldos de los trabajadores? No, verdad? Porque eso es vital. Además, saben que no pueden dejar de pagar la luz, porque eso también es vital. Cuando la Alta Dirección entienda que la seguridad de la información es vital, entonces asignarán automáticamente un presupuesto para seguridad, automáticamente un presupuesto para personal de seguridad, automáticamente consultorías, controles, etc.

Yo: ¿El oficial de Seguridad está como un personal permanente o no?
E: No hay un Oficial de Seguridad de las estructuras orgánicas. Generalmente los Oficiales de Seguridad son CAS. Es decir que no son permanentes.

Yo: ¿Eso sería otro problema?
E: Claro, pero eso ya es una cuestión más de trámite. Que se podría solucionar una vez que se avance en otros temas. Porque, ¿Quién va a crear el perfil del oficial de seguridad? Se lo tiene que crear el mismo oficial de seguridad, ya que las otras personas no saben de seguridad. Entonces, ¿cómo van a generar un perfil de oficial de seguridad de información?

Yo: Respecto de la Alta Dirección, Ud. me dice que ellos tienen claro la importancia de implementar el SGSI en su institución, entonces ¿deberían tratar de asignar presupuesto?
E: Es por eso que digo que la Alta Dirección saben de su importancia, porque se les ha ido concientizando, pero todavía no lo asocian a un asunto de presupuesto.

Para poner un ejemplo práctico, es como decir: "*Los niños en el Perú necesitan leer más*". Todos sabemos que es importante que las personas lean más. Es importante porque tendríamos una mejor calidad de seres humanos si todos leyeran más. Todos sabemos eso. ¿Cuántos de nosotros se sientan con algún niño que tiene en casa a leer?

Es más o menos eso, la Alta Dirección sabe que es importante la seguridad de la información. Se les ha explicado los problemas, los riesgos, la necesidad y la importancia; pero, al momento de tomar decisiones, hay prioridades que ellos sienten más en la piel que las de seguridad de información.

Yo: Pero la Alta Dirección ¿Si da el respaldo para el desarrollo del SGSI?
E: Eso sí. En mi caso específico, no me dan presupuesto pero yo tengo un gran respaldo. Digamos que el oficial de seguridad es importantísimo, él determina que información se da y que información no. Si hay alguna duda respecto de la normativa de seguridad, a la ley de protección de datos personales, si se debe entregar información o no, todo se pide opinión del oficial de seguridad. El hecho de que pidan la opinión del oficial de seguridad le da importancia a esa función. Y de alguna manera por la explicación que da el oficial de seguridad van a tomar conciencia de porqué esa información puede servir, porqué ese procedimiento no se

debe hacer, porqué tendrían que tener cuidado con tal o cual cosa. Es una forma de generar confianza y empoderar al oficial de seguridad.

Yo: ¿Y hay reuniones periódicas del oficial de seguridad con el comité de seguridad?
E: Si, se reúnen cada mes. Se hacen actas, se toman acuerdos.

Yo: En estos comités se designan a los altos cargos, pero a veces para las reuniones mandan a otras personas de rango inferior. En el caso de su institución ¿Sucede esto?
E: Felizmente no. Por ese lado, están concientizados. Van todos a la reunión del comité de seguridad de la información.

Yo: ¿Y fue difícil crear el Comité, hubo trabas allí?
E: Tengo que reconocer que mucho hace la buena relación que haya entre los altos directivos, para este tipo de iniciativas. Mucho hace la llegada que tenga el gerente de TI ya que el oficial de seguridad está dentro de la gerencia de TI. El gerente de TI de ese momento tuvo una gran influencia para convencer y crear el comité.

Por eso digo, la piedra angular es el respaldo de la Alta Dirección. Si a él no le hubieran hecho caso o si hubiera tenido él rencilla con el gerente general o con alguno de los gerentes que conforman el comité de seguridad, se hubieran opuesto a las medidas porque finalmente somos todos seres humanos.

Yo: Da la sensación de que el área de TI esté llevando a cabo esta implementación, ¿Ud. está de acuerdo con que el oficial de seguridad esté en el área de TI?
E: Sí y no. Para una entidad donde en ningún momento anterior se ha abordado el tema de seguridad y teniendo en cuenta que la cuestión más tangible de seguridad actualmente está en los sistemas informáticos, y teniendo en cuenta además que seguridad para que sea seguridad primero tiene que exculcar y ver que se está haciendo mal, es necesario que esté dentro de TI. Si es que estuviera fuera de TI nadie va a decirle, siendo también realistas, cuales son las falencias de un área ya que todos vamos a querer dar una buena imagen hacia afuera.

En buena cuenta, el oficial de seguridad es como un auditor que va a revisar que se está haciendo y como nadie va a querer quedar mal -porque es la naturaleza de las instituciones públicas- ante otra área y van a maquillar las cosas, va a cubrirlas ya que si no podría peligrar su puesto; más aun sabiendo que esa información va a la Alta Dirección.

A mi parecer una buena estrategia es que, inicialmente, seguridad de la información esté en el área de TI para que seguridad, estando dentro, pueda arreglar la casa. Arreglar por lo menos el área de TI que es el área neuronal y neurálgica donde actualmente se encuentra la información de cualquier institución. Posteriormente, como parte de la maduración organizacional, ya seguridad de la información pasará a otra área sabiendo cómo es que funciona TI, sabiendo cuáles son sus fortalezas, sus falencias, qué tiene que buscar, donde tiene que buscar. Personalmente, pienso que como inicio en una organización es bueno que seguridad de la información esté en TI.

Yo: Respecto a la capacitación en SGSI, ¿La institución da capacitación en seguridad al oficial, a la gente que interviene o al comité mismo?
E: No. Ya últimamente ha habido un curso después de mucho insistir. Lo que pasa es que también no es solamente en el tema de seguridad de la información.

En general no se capacita, no hay una cultura a nivel de las instituciones públicas de capacitar al personal, porque además tienen el presupuesto limitado y no hay la cultura de invertir en capacitación.

Yo: Su institución trabaja a nivel nacional, ¿la seguridad de información está centralizada sólo en Lima?
E: Se establecen las bases aquí y se tratan de replicar a las provincias en la medida que se pueda.

Yo: ¿Y en las provincias se tiene personal de seguridad de información?
E: No, no se tiene. Lo que pasa es que seguridad de la información es transversal a toda la institución. En seguridad de la información tiene que estar inmersos desde el vigilante de la puerta hasta el gerente general.

Yo: ¿La estructura organizacional actual favorece el desarrollo de la implementación de seguridad de la información?
E: Como dijimos inicialmente, la implementación del SGSI según la NTP 27001, está orientada a una organización por procesos. Nuestra organización es funcional. Ahí hay un conflicto, un escollo que tenemos que idear la forma de poder hacer la implementación.

Yo: ¿Y qué metodología de gestión de riesgos vienen aplicando?
E: Teniendo en cuenta que es la primera vez que se hablaba de riesgos, que no había personal; Por lo tanto, la evaluación de riesgos yo sola no podía hacerla para las 03 gerencias que involucra el área de TI, la evaluación de riesgos tenía que hacerlo con la participación y colaboración de las mismas áreas. Por ello, no podía implementar una metodología de riesgos tan profunda como Magerit, como Octave, porque habría que capacitar y en hacer esa inmersión a todas las personas de las otras áreas para que ellos puedan hacer un análisis de riesgos en función de esas metodologías.

Por tanto, se optó por utilizar una metodología sencilla y básica como lo han hecho muchas instituciones, como el BCR, que nos permita identificar unos riesgos iniciales sobre los cuales se puedan trabajar y mitigar e ir mejorando el siguiente año. Como esto es un ciclo de mejora continua, el próximo año se puede mejorar la metodología, ampliar los parámetros. Lo importante es empezar.

Pero hemos iniciado de lo básico como para que todos puedan entender cuál es el riesgo que tienen y cómo tienen que mitigarlo.

Yo: ¿Y hay una cultura organizacional del SGSI en el personal de su institución?
E: Cuando la persona que tiene encomendada una misión que involucra a las demás, está demasiado empoderada, la gente cumple.

Yo: ¿Pero el personal de su institución tiene una real conciencia del SGSI?
E: Por lo menos en el área de TI ha funcionado, yo he notado muchos cambios de cuando llegué respecto al cuidado de la información.

Yo: ¿Ha sido difícil la implementación del SGSI en su institución?
E: En el área de TI no ha sido tan difícil, por un lado porque tenía el respaldo del jefe inmediato que es el gerente de TI. Formalmente él envió un comunicado a las 03 gerencias diciendo que yo era el oficial de seguridad y que en buena cuenta tenían que hacerme caso.

Yo: ¿Y con respecto a la concienciación del SGSI en las demás áreas de la institución?
E: En algunas áreas si lo hay y en otras áreas no la hay. En realidad mucho depende cuando el contacto ha sido directo con el gerente general que era el que me daba el espaldarazo para que yo pueda actuar. Por ejemplo, se dieron unas charlas de sensibilización en cada área y donde iban a enfocarse en las debilidades de seguridad de información de cada área, ya que lo que es importante para finanzas tal vez no lo es para personal. Entonces yo empezaba visitando un área, identificando las falencias de información, primero hablaba con el gerente y le explicaba cuál era mi función y le explicaba que yo iba a hacer un análisis previo de su área, que se lo iba a alcanzar para que él pudiera mitigar esos riesgos y que luego yo iba a dar una charla para todo su personal señalando las debilidades que ellos tenían que superar y los riesgos a los que conllevaba esa identificación.

Eso me funcionó muy bien porque en las instituciones públicas tenemos 02 situaciones: la respondabilidad ([1]) y la responsabilidad. Tenemos que dar cuenta de lo que nos han asignado y somos responsables de lo que hacemos. Si a alguien le dices: "mira, hay cosas que no te das cuenta" por el día a día o porque siempre lo has hecho así y podrías estar incurriendo en algo que es tu responsabilidad y no lo estás haciendo. Y te lo voy a decir como si fuera una auditora, sin serlo, y te voy a evitar un dolor de cabeza con los auditores o con los jefes inmediatos.

Esa estrategia es una buena forma de ganar la confianza, sobretodo porque cuando ganas esa confianza, las personas de mando medio y las personas operativas vienen y me cuentan en la oficina sobre lo que está pasando y si es peligroso o riesgoso. Como no es oficial, hay menos temor y uno funge de sacerdote que escucha las confesiones y eso te sirve para poder dar opciones de mejora. Eso a mí me ha funcionado muy bien.

Yo: ¿Y en la institución hay algún plan de concienciación de seguridad de la información al personal?
E: Sí, se ha elaborado un plan de sensibilización de seguridad de la información que abarca en la 1ra. Etapa todo Lima centro, que son 3,500 personas. La 2da. Etapa que incluye los conos de Lima y la 3ra. Etapa a nivel nacional. Este plan involucra todo un conjunto de actividades.

Una de ellas es la de sensibilización por popups. Es decir cuando prendes tu máquina aparece un mensaje. También hay charlas, y se ha considerado que nadie va a una charla de algo que no sabe de lo que se trata. Se han considerado incentivos

como cuadernitos, pad mouse, etc. para que vayan a la charla. Así también se ha creado una página web de seguridad de la información que está dentro de la intranet a través de un icono de seguridad de la información que cuando haces clic aparece una presentación del oficial de seguridad, con los puntos principales de porqué es importante la seguridad, hay algunos videos y las normativas que se están aprobando.

Yo: ¿Qué factores entonces cree Ud. que impactan o impiden la implementación del SGSI en las instituciones de la administración pública?
E: Si hubiera una concientización, una sensibilización a la Alta Dirección; ellos tomarían todas las medidas necesarias: contratarían personal, asignarían recursos, controlarían. Pero esa concienciación no es solamente de la institución, porque esa sensibilización tendría que tenerla también el titular de todo el pliego; es decir, una concientización de una gran cabeza hacia las cabezas se podría tener más fuerza.

Lo que hace ONGEI es la concientización y el apoyo a los oficiales de seguridad, pero estos oficiales son del mando medio, ellos tienen que estar solicitando a un mando mayor sus requerimientos de recursos. Si bien uno de los pilares del gobierno electrónico es la seguridad de la información habría la necesidad de un mecanismo que no sea de abajo hacia arriba, porque es el oficial de seguridad el que tiene que convencer a la Alta Dirección, cuando debería ser alguien que esté más arriba y decirle a los de la Alta Dirección de las instituciones públicas que este tema es importante. Actualmente, la ONGEI llega a los oficiales de seguridad y a los gerentes de TI, pero estos no son decisores, no otorgan recursos.

Para mí este tema es básico, es como el fluido eléctrico. ¿Acaso hay charlas de sensibilización del fluido eléctrico sobre su importancia? No, no hay charlas. Porque todos saben que tienen que pagar la electricidad, porque puede incluso faltar agua pero sin la electricidad no se podría trabajar. Cuando la Alta dirección de las instituciones públicas piense así de la seguridad de la información, no va a ser necesario pedirles recursos ya que ellos nomás van a saber que necesitan asignar recursos, necesitan capacitar a la gente en este tema.

Yo: ¿Algo final que quiera agregar para finalizar la entrevista?
E: Yo creo que estamos avanzando, debemos ver los inicios no como lo mucho que nos falta sino como lo importante de haber empezado. Normalmente yo escucho que aún nos falta un montón, que estamos en nada, que para cuándo será; pero yo creo que si en lugar de pensar así decimos “hemos empezado”. Tanto tiempo que hemos estado sin este cuidado y ahora que hemos empezado, que bueno, de aquí sólo nos queda avanzar. Una vez que empiezas sólo te queda avanzar hacia adelante ya no puedes retroceder, darle fuerza a esta política.

(1) Actualmente se ha comenzado a utilizar el término “respondabilidad” (“accountability” en inglés) para transmitir los conceptos que el término inglés conlleva: responsabilidad ante la comunidad, rendición de cuentas que no sean necesariamente en dinero, y compromiso moral y legal ante otros.

ANEXO 13: TRANSCRIPCION DE LA 6ta. ENTREVISTA

La entrevista está dividida en 03 partes:

La primera tiene que ver con la parte más técnica, es decir con la experiencia laboral y personal que Ud. tenga con respecto a la seguridad de información. Una segunda parte normativa, que son preguntas referidas a la misma norma y con la ONGEI misma que es el ente que norma este proyecto. Y una tercera parte operativa, que son preguntas del SGSI en su Institución, es aquí donde desarrollaremos más profundamente el tema de la tesis de investigación

Respecto de la Dimensión Técnica:

Yo: ¿Cómo define Ud. lo que es un Sistema de Gestión de Seguridad de Información?
E: Bueno un sistema de gestión de seguridad de información se refiere a todos los mecanismos y actividades que una entidad debe considerar para poder asegurar la información en sus diferentes aspectos, no necesariamente en lo tecnológico; sino también en lo físico, como por ejemplo dejar un documento encima de un escritorio que es también seguridad de la información.

Es decir, cómo resguardar que la información de una entidad no se vea perjudicada por actividades que no son seguras.

Yo: ¿Qué experiencia personal o profesional tiene Ud. respecto de la seguridad de información?
E: Bueno. Actualmente soy Oficial de Seguridad de Información en el Ministerio de Economía y Finanzas desde el año 2012 aproximadamente. También he sido Director general de la Oficina de Tecnologías de Información, conozco los procesos que se dan en dicha Oficina principalmente de los procesos operativos que son los que más están ligados a los riesgos de seguridad.

Yo: ¿Ud. pertenece o ha pertenecido a alguna asociación vinculada a la seguridad de información?
E: Bueno, pertenezco a las que son parte del Estado como son el PeCERT. También he participado como miembro del CODESI a en la PCM haciendo el Plan de la Sociedad de la Información, tanto en su 1ra. versión como en su 2da. versión.

Respecto a la Dimensión del Proyecto, es decir preguntas técnicas referidas a la norma técnica 27001:

Yo: ¿Para Ud. qué es la Norma Técnica Peruana 27001 y qué papel cumple la ONGEI en la implementación de esta norma?
E: Bueno, la NTP 27001 es una norma que de alguna manera trata de aplicar en el Perú lo que es el estándar mundial de seguridad el ISO 27001, y está promovida por la ONGEI que es el ente rector de gobierno electrónico e informática para la seguridad del Estado.

Yo: ¿Cree que viene cumpliendo su papel?

E: Si está tratando de cumplir su papel, lo que le falta es un poco más de respaldo político puesto que es una oficina informática que depende de la Presidencia del Consejo de Ministros (PCM).

No es una oficina con representatividad política propia, no tiene la fuerza suficiente para la ejecución de las normas que dicta.

A pesar de ello, viene implementando muchas actividades o acciones orientadas al gobierno electrónico y al desarrollo de las entidades en ese aspecto.

Yo: ¿Cree que (ONGEI) logra su cometido de articulación de las entidades públicas?

E: Más que articularlos, yo diría que los concentra y hace que se guíen bajo un mismo objetivo y un mismo horizonte. Por ejemplo, en el tema de la obligatoriedad del Plan Estratégico de Gobierno Electrónico (PEGE) hace que todas las entidades definan ese plan, definan actividades orientadas más al servicio de seguridad de la información. El problema es que ONGEI es una entidad pequeña, le falta la fuerza como para que dirija y oriente con mayor fuerza a las entidades del Estado.

Yo: ¿Qué objetivos cree que busca el Estado Peruano con la implementación de esta norma?

E: Lo que busca es minimizar los riesgos en el uso y manejo de la información en las entidades públicas. Actualmente, hay muchas entidades que por desconocimiento de los procesos que tienen no resguarden bien su información, no la protejan. Entonces, esta norma trata de que todas las entidades realicen actividades de seguridad de una manera estándar para que sigan lineamientos que les permita proteger su información en diferentes aspectos en los 11 dominios que dice la norma.

Yo: ¿Qué factores cree Ud. que vienen influyendo en el Estado en la implementación de la NTP 27001?

E: Uno de los factores que viene influyendo es el entendimiento que puedan tener las áreas no informáticas de la entidad y la Alta Dirección de la misma para apoyar a la Oficina de Informática para que se desarrolle esta norma.

Por ejemplo, como esta norma es de obligatorio cumplimiento por parte de las entidades públicas, la mayoría piensa que es un tema informático únicamente y no es así. Entonces, no les dan el apoyo necesario ya que requiere un presupuesto adicional para cubrir algún riesgo o comprar un equipo o firewall nuevo, un equipo de seguridad perimetral, y si no le dan el presupuesto requerido entonces ese control que exige la norma que hay que aplicar, no se puede dar o demora mucho tiempo en aplicarlo. Entonces, primero tiene que haber un entendimiento de la Alta Dirección de la importancia que tiene esta norma.

Yo: ¿Tiene Ud. conocimiento de normas técnicas anteriores a la NTP 27001?

E: Lo que te puedo decir es que todos los estándares ISO 27000 son todos relacionados a seguridad de información, pero aplicadas en el extranjero. Aquí en el Perú, se empezó con la 17799 que era una metodología de seguridad; luego salió la

27001, para que se tengan las pautas de cómo hacer las cosas y luego ya recién ejecutarlas.

Yo creo que ONGEI ha hecho un buen trabajo con todo esto porque las entidades de por sí nunca lo iban a aplicar. Es decir, si cada una definía por sí misma como proteger su seguridad, no iban a cubrir todos los ámbitos que pide la norma. Esto ha llevado a muchas entidades a contratar un servicio de análisis de riesgos para poder identificar brechas.

La entidad muchas veces no tiene la justificación para implementar la seguridad de información, entonces con esta norma se ha permitido justificar que se necesita un análisis de brecha en cuanto a seguridad.

Yo: ¿Y tiene conocimiento de algún caso de éxito de alguna entidad que haya implementado la NTP 27001?
E: Sé que ya existen varias entidades que han cumplido el 1er. ciclo de implementación de la norma, incluso ya se han certificado, como en el caso de la ONP; pero en diferentes ámbitos, ya que la norma permite certificar procesos, áreas o entidades.

Yo: ¿Quiere decir que no hay un estándar de implementación?
E: La norma permite, como es un ciclo de mejora continua, empezar por partes e ir creciendo. Entonces, cuando es una entidad pequeña de repente se podría implementar la norma en toda la entidad porque tienen procesos pequeños, pero en entidades grandes conviene más empezar por partes.

Yo: Hace poco se ha aprobado la NTP 27001:2014 ¿Cree que esto beneficiará más la implementación en el Estado?
E: Yo creo que sí, ya que me da mayores pautas y amplía un poco más la 27001:2008. Pero en sí es el mismo espíritu de mantener el control de todos los riesgos que puede haber en cuanto al manejo de la información de la entidad en sus diferentes aspectos.

Respecto a la Dimensión Institucional, es decir preguntas referidas a la seguridad de la información en su institución:

Yo: ¿Cómo cree Ud. que viene beneficiando en su institución la implementación de la Norma Técnica 27001?
E: La aplicación de la norma 27001, en la institución donde trabajo ha permitido identificar algunas acciones que faltaban realizar. Usualmente, por ejemplo, uno se basa en procedimientos operativos pero a veces hace falta también procedimientos normativos que aseguren o guíen el correcto uso de la información.

Entonces, al revisar la norma y revisar los controles se identifican que hay varias acciones que faltan realizar. Por tanto, las instituciones con la norma tienen una guía para -en base a los controles que hay que cumplir- planificar todas las acciones que hay en el corto, mediano o largo plazo para asegurar que los procesos sean correctos y con calidad.

Ahora, hay muchos procesos que también escapan de lo tecnológico y se requieren coordinaciones con otras áreas. Entonces, allí también hay temas de educación con las otras áreas o de coordinación muy extensa para que estas áreas entiendan que la aplicación de la norma va más allá de lo tecnológico.

Por ejemplo, uno de los controles que se detectó en la institución donde trabajo es que no había mucha seguridad en el acceso físico de las personas, es decir que no a todas se les daba fotocheck, de tal forma que las personas conocidas pasaban sin que se les dé ninguna identificación. Entonces con el control indicado en la norma, se coordinó con la oficina de administración para que así sean personas contratadas que ya son conocidas que vienen todos los días pero que tienen una modalidad de contrato que no usan fotocheck, se les otorgue el mismo y por otro lado que vigilancia también controle estrictamente que nadie que no tenga credencial ingrese a la entidad, así sean personas de la entidad o las visitas también se les provea uno.

Yo: ¿O sea que ha beneficiado, en el sentido de haber mayor seguridad?
E: Claro, hay más seguridad, más orden, hay más controles.

Yo: ¿En su institución existe el apoyo de la Alta Dirección para la implementación de la NTP 27001?
E: Sí, hay ese apoyo. Y eso se nota ya que el comité de seguridad de la información está conformado por Directores Generales, la Secretaría General y el Director de Riesgos Operacionales que pertenece al área de Tesoro Público que aporta mucho para poder ver los riesgos a nivel institucional, también está el jefe de la Oficina General de Administración, que ve el tema de RR.HH. y administrativos, también el jefe de la Oficina de Planificación y Presupuesto.

Yo: ¿Y en qué nivel o fase de la implementación incremental de la norma se encuentran?
E: Estamos ya en la fase final, es decir en la quinta etapa. Ya estamos culminando las actividades del plan de seguridad de información que se aprobó para este año. Tenemos planificado culminar las actividades del plan a fines de octubre y luego volver a hacer un análisis de riesgos, identificando nuevos riesgos y, si los hubiera, empezar nuevamente todo el circuito de la NTP 27001.

Yo: ¿Tienen pensado Uds. certificarse?
E: Claro, la intención es certificarnos. Si pasamos todos los controles con el análisis de riesgos que vamos a hacer yo creo que estaremos en capacidad de certificarnos.

Yo: ¿Cuál es el Alcance que han definido?
E: El Alcance es todos los procesos de la Oficina General de Tecnologías de Información, dado que los procesos que soporta la oficina son procesos transversales a toda la institución. Tanto el soporte técnico, el mantenimiento de los sistemas que usa toda la entidad y que, al asegurar la información de los sistemas y de los procesos, estamos asegurando la información que manejan todas las demás dependencias del ministerio.

Yo: ¿Este Alcance ha costado definirlo?
E: Bueno, para que los miembros del comité de seguridad de información entiendan primero lo que significaba la norma hubo muchas reuniones de coordinación y de explicación; luego, para hacerles entender que el ámbito debería ser la oficina de tecnologías de información también ahí hubo que hacerles entender el porqué.

Muchas áreas de línea pensaban que debían ser ellas a las que se les identificaran los riesgos de su área por ser de mayor importancia. Por otro lado, la oficina de tecnologías de información está catalogada como una oficina de apoyo en el ministerio y es por ello que pensaban que la importancia de esta oficina era menor. Sin embargo, dados los procesos que son transversales, todos los procesos donde todo está tecnificado y todo tiende a automatizarse, entonces se aprobaron que el alcance sea a todos los procesos de la oficina.

Yo: ¿Y este Alcance del SGSI solamente es al Data Center?
E: No, es a toda la oficina. Es decir, todos los procesos que realiza la OGTI, llámense los procesos del área de sistemas de información, el área de infraestructura tecnológica que es la que da soporte a todos los equipos hardware y software, y el área de Gobierno de Tecnologías de Información que es el área que define todos los procesos, los procedimientos, las estrategias y los proyectos de TI.

Yo: ¿Qué estructura organizacional tienen instalada en su institución respecto del SGSI?
E: Tenemos un comité de gestión de seguridad de información y debajo de ello hay un comité técnico que está conformado por personal de la oficina de tecnología de información.

Yo: ¿Tienen asignado un presupuesto de forma exclusiva para la implementación del SGSI?
E: En un principio no se tuvo, pero luego cuando ya se aprobó el plan de seguridad de la información del presente año (2015) y, al haber sido aprobado por todos los miembros del comité de seguridad, se le buscó un presupuesto. El plan se desarrolló a fines del año pasado y se logró incluir en el presupuesto anual las actividades que requerían presupuesto

Yo: ¿Y antes de este año, cómo manejaban algún presupuesto para el SGSI?
E: Antes de este año utilizábamos presupuesto de la OGTI, se cubrían actividades del SGSI con presupuesto de la oficina de TI, lo cual restaba recursos al área y no se podían desarrollar las actividades del SGSI en el tiempo previsto porque era un presupuesto inseguro. Tenían que dejarse de hacer unas cosas en TI para poder ejecutar estas acciones de seguridad que eran prioritarias también, pero a veces esto no alcanzaba. Por eso se aseguró el presupuesto para SGSI este año.

Yo: ¿La Alta Dirección ha dado el apoyo necesario para el desarrollo del SGSI?
E: Bueno, esto ha sido parte del proceso de concientización de las personas que no están relacionadas con la norma, de hacerles entender que muchas de las adquisiciones de tecnología requeridas eran necesarias para cumplir con los controles de seguridad de la norma.

Muchas veces se cree que al comprar un firewall o un software de encriptación son simplemente para mejorar los procesos tecnológicos, pero en este caso son para mejorar la seguridad de la información en los servicios que se brinda.

Al inicio del entendimiento, cuando comenzamos a implementar la norma se pensaba que esta era sólo de aplicación tecnológica y que era la OGTI la que debía correr con los recursos propios de tecnología.
Pero después cuando se fue entendiendo la magnitud y la implicancia, los miembros del comité de seguridad tomaron conciencia de que es un tema institucional y no solamente tecnológico y se aperturaron las facilidades para conseguir un mayor presupuesto.

Yo: ¿Cree que la Alta Dirección tiene clara la importancia de implementar el SGSI?
E: Yo creo que ahora si lo tienen, ya que ahora se hace un seguimiento constante. Cualquier tema relacionado con el SGSI, el comité se reúne y está muy interesado en saber el avance de las actividades.

En un principio, por las mismas etapas que tiene el ciclo de vida de la norma, una de las primeras fases era hacer un análisis de riesgo, definición del alcance, identificación de los controles, actividades que mitiguen los riesgos; toda esa parte era cómo de análisis. Ya cuando producto de ello, se determina el plan de acción es que ya comienzan a salir actividades concretas que son visualizadas por el comité: que el personal use fotocheck, procedimiento para que el personal ya no deje los documentos en su escritorio, que cuando todos se vayan desenchufen sus equipos de cómputo; entonces, ya se fueron identificando acciones que no sólo son de TI, sino que ya dependen de administración o de hasta secretaría general.

Yo: ¿Ud. cree que aplicar en la organización un tema como ISO 9001 o calidad de procesos es necesario, es importante o no?
E: Yo creo que sí. El ISO 9001 asegura la calidad de los procesos durante todo el ciclo del mismo. Sin embargo, en nuestro caso, cuando apareció la norma, tuvimos que aplicarla con los procesos que teníamos, ya que si esperábamos a certificar primero un proceso y madurarlo así como lo pide un ISO 9001, íbamos a esperar mucho y los riesgos que pueden presentarse son muy peligrosos.

Yo creo que con el análisis de riesgos que se hizo se identificaron las brechas que existían entre lo que pide la norma, lo que uno debe tener versus lo que uno tiene, entonces ahí se identificó que cosa le faltaba a los procesos que teníamos.

Yo: ¿Ese análisis de brecha, Uds. lo tercerizaron con algún tercero?
E: Si. Lo realizamos con una empresa especializada en seguridad de información que hizo este análisis de brecha, el cual demoró cerca de 6 a 7 meses con un diagnóstico detallado y nos dejó plantillas de procesos, entre otras cosas.

Yo: ¿Osea que si bien no se aplicó el ISO 9001 por el tema del tiempo, si se aplicó otra metodología como fue el análisis de brecha?
E: Así es. Ellos trajeron su propia metodología de análisis de brecha ya madura. Con eso nos dejaron indicaciones de cómo seguir actuando para cumplir con la norma y sobre qué procesos además. En la OGTI se identificó qué procesos estaban débiles, qué procesos le faltaban documentar.

En resumen, este análisis nos ayudó a identificar nuestras debilidades. Esta empresa nos sugirió incluso qué hacer para mejorarlas, nos dieron los lineamientos. Incluso el alcance del SGSI fue sugerido también por ellos aprobado luego por el comité de seguridad.

Yo: ¿Ud. está de acuerdo con que el área de TI sea la encargada de implementar el SGSI?
E: Si estoy de acuerdo, porque de alguna manera porque muchos de los controles van a recaer en procesos sistematizados. Asimismo, las operaciones de las demás áreas también están automatizadas y sus controles también lo están. Por tanto, las vulnerabilidades, los riesgos, la falta de controles tienen que revisarse en base a los sistemas informáticos que se utilizan; y si alguien audita al área de tesorería o presupuesto por ejemplo, le va a auditar el sistema informático que utiliza: que seguridad tiene ese sistema que usa, como están automatizados sus procesos y la OGTI se va a ver obligada a revisar esas vulnerabilidades también en dichos sistemas.

Yo: ¿Entonces cree que la estructura organizacional de TI favorece el desarrollo del proyecto del SGSI?
E: Yo creo que sí. Pero eso también es porque en la institución la oficina de TI es una oficina general, a pesar de ser un órgano de apoyo está a nivel de línea. En cambio, hay otras instituciones del Estado en que su oficina de informática está dentro de la oficina de administración, y ahí no tiene el peso necesario para poder coordinar o sugerir la aplicación de un procedimiento o de un control; no tiene la fuerza ya que tiene que depender de un jefe superior, y si este jefe su negocio principal es la administración y no la tecnología, entonces no le va a dedicar el esfuerzo necesario que si fuera el mismo director de tecnología que va a aplicar la norma y luchará por eso.

Yo: En el tema de la capacitación, ¿Recibe o ha recibido capacitación sobre seguridad de información?
E: Bueno, como parte del servicio que se contrató para el análisis de brechas, hubo talleres de capacitación en lo que es seguridad de información. También en talleres que ha promovido la PCM a través de la ONGEI.

Además, en el área se han realizado talleres de capacitación para el personal de la oficina de TI, tanto para los desarrolladores, operadores, directivos. A nivel institucional se ha realizado talleres de sensibilización de seguridad de la información a todo el personal para que sepan primero que cosa es seguridad de información diferenciándola de seguridad informática, y que lo repliquen en sus oficinas y hasta en sus hogares.

Yo creo que entendiendo el concepto, este va a ser el punto principal para que, a partir de allí, exista el apoyo necesario de todos los trabajadores de la institución en seguir los lineamientos que dice la norma.

Yo: ¿Y qué metodología de gestión de riesgos vienen aplicando? ¿Cómo se determinó?
E: Cuando se hizo la consultoría, justamente recién se creaba la oficina de riesgos de la institución que depende de otra oficina general, donde ellos habían hecho una

metodología de riesgos operacional. Por otro lado, la empresa consultora trajo su propia metodología de riesgos. Entonces, a efectos de no tener dos metodologías distintas se validaron ambas metodologías, determinándose que la metodología de riesgos de la empresa consultora si era aplicable y coincidía mucho con la de la oficina de riesgos recién creada, aprobándose la misma.

Yo: ¿Y hay una cultura organizacional del SGSI en el personal de su institución?
E: Bueno, los talleres de sensibilización desarrollados han tenido efecto, ya que hemos sido bastantes didácticos explicando los diferentes riesgos existentes de no cuidar la información que manejan. Incluso, hace poco hemos realizado una inspección de las oficinas para ver si alguien deja expuestas sus claves por ejemplo, para ver si existen riesgos, y no hemos encontrado mayor problema.

Yo: ¿Existe un programa de concientización del SGSI al personal de su institución?
E: Según nuestro plan de seguridad de información, está definido que se dicten charlas periódicas de capacitación al personal de la institución en forma semestral, cada 06 meses.

Normalmente, contratamos una empresa especializada que venga con un temario bien definido incluyendo afiches para su difusión referidos a la seguridad de información con diferentes tips: "no deje prendida su computadora cuando se vaya", "no deje su usb en su escritorio cuando su oficina está abierta", "no deje sus claves escritas", etc.; que luego son pegados en toda la institución.

Así también vía correo se pasan estos mismos tips a los trabajadores como mensajes recordatorios.

Ahora, como parte de la NTP del SGSI también se implementó una política de seguridad de información de la institución que ha sido la base para tomar algunas acciones de seguridad y, en su momento, también fue difundido al personal cuando se aprobó y se difundió por correo.

Pienso que todo esto que se ha desarrollado, como le pasa también a otras entidades públicas, es bastante nuevo en la implementación de la NTP y ya en un segundo ciclo se hará con mayor conocimiento y hasta con mejoras, haciendo más sólidas las cosas. Tal vez incluyendo una intranet quizás donde existan boletines de seguridad por ejemplo. Incluso ya habrán procesos más definidos, etc.

Yo: ¿Qué otros factores cree Ud. que impactan o impiden la implementación del SGSI en las instituciones de la administración pública?
E: Uno de los factores que afectan es el tiempo que toman los procesos de adquisición de los elementos que se requieran para el plan de seguridad de información sobre todo cuando son complejos o de montos altos. Por ejemplo, si se identifica que se requiere encriptar los correos por un tema de seguridad o se requiere mejorar el firewall o comprar uno nuevo, si es que no estuviera presupuestado, todo el trámite que lleva para presupuestarlo es muy engorroso y, si además dicho proceso queda desierto, hay que volver a convocar y así pueden pasar

varios meses. Estos riesgos son los que a veces dilatan el cumplimiento de la norma en los plazos previstos.

Pienso que una de las cosas que debería hacerse es que las adquisiciones por temas de seguridad de información deberían tener un marco legal diferente, exonerarlos tal vez de algunos procesos o de menor tiempo en sus plazos, siendo totalmente transparente con las convocatorias respectivas eso sí.

Otro problema que se ha presentado también es que para cumplir las actividades del plan de seguridad de información y que involucra a otras áreas, a veces hay que lidiar con el plan de trabajo de esas áreas que ya lo tienen definido. Y cuando uno viene con una actividad adicional, que salió producto de la identificación de algún riesgo, les cuesta incorporarlo en su plan. Entonces uno tiene que estar insistiendo e insistiendo para realizar el mismo y se dilata el tiempo y plazo que se tiene para su ejecución.

Yo: ¿Algo final que quiera agregar para finalizar la entrevista?
E: Bueno, creo que atacar un tema como es la seguridad de la información es bastante importante y es bastante útil ya que ello no es por épocas, ni que se hace en un momento determinado y ya no se hace después, sino que es algo que se hará permanentemente y con la tecnología además que avanza muy rápido y las vulnerabilidades o los intentos de robo de información son cada vez más constantes sobre todo a los portales de las entidades públicas por lo que siempre tienen que estar preparadas con sus controles de seguridad actualizados.

Anexo 14: TRANSCRIPCION DE LA 7a. ENTREVISTA

La entrevista está dividida en 03 partes:

La primera tiene que ver con la parte más técnica, es decir con la experiencia laboral y personal que Ud. tenga con respecto a la seguridad de información. Una segunda parte normativa, que son preguntas referidas a la misma norma y con la ONGEI misma que es el ente que norma este proyecto. Y una tercera parte operativa, que son preguntas del SGSI en su Institución, es aquí donde desarrollaremos más profundamente el tema de la tesis de investigación

Respecto de la Dimensión Técnica:

Yo: ¿Cómo define Ud. lo que es un Sistema de Gestión de Seguridad de Información?
E: Un Sistema de Gestión de Seguridad de la Información es un conjunto de factores o normativas que me van a ayudar a enseñar y motivar al uso de ciertas herramientas para que las personas de la organización puedan utilizar, de manera proactiva, los instrumentos que tienen en sus oficinas para gestionar de una mejor manera su información sobre todo la más crítica.

Por tanto, vendría a ser todo un conjunto de políticas y normas que van a ayudar a fomentar la seguridad de la información y que tengan mucho más cuidado en su tratamiento.

Yo: ¿Qué experiencia personal o profesional tiene Ud. respecto de la seguridad de información?
E: Bueno, yo tengo un año como oficial de seguridad de la información implementándolo en la entidad que laboro. Se inició primero como un proyecto piloto en un museo con la norma anterior (la NTP-ISO/IEC 27001:2008). Esta norma estaba ya casi implementada en dicho museo y ahora estamos actualizándola toda la documentación a la 27001:2014.

Finalmente, a finales del 2015, se llamó a una empresa certificadora para que nos hiciera una pre-auditoría y que nos evaluara como estábamos con la implementación de la norma ya que no teníamos tanta experiencia en esto. Esto nos arrojó como resultado que tenemos unos buenos índices en lo avanzado pero con algunas observaciones que son viables de resolver

Yo: ¿Ud. pertenece o ha pertenecido a alguna asociación vinculada a la seguridad de información?
E: No, no pertenezco a ninguna asociación de seguridad de la información. He llevado algunos talleres relacionados principalmente con ONGEI y en la maestría.

Respecto a la Dimensión del Proyecto, es decir preguntas técnicas referidas a la norma técnica 27001:

Yo: ¿Para Ud. qué es la Norma Técnica Peruana 27001 y qué papel cumple la ONGEI en la implementación de esta norma?
E: Bueno, como se sabe la NTP recién ha sido aprobaba en enero de este año. Por tanto, ha sido muy importante que se dé esta norma ya que muestra una mejor visión de lo que estamos haciendo respecto al año anterior.

Ahora, esta nueva norma ha tenido un gran cambio respecto a que se puede implementar sobre cualquier entidad y en lo que respecta a su organización. Por tanto, tuvimos que sacar una resolución del comité de seguridad con la definición (como dice la norma) de los integrantes de la misma.

La ONGEI está cumpliendo un papel fundamental en lo que respecta a la fomentación de la implementación de esta norma sobre todo porque ellos vienen brindando un apoyo técnico. Incluso nosotros ya lo hemos solicitado y estamos a la espera de su respuesta.

Yo: Con la norma anterior (27001:2008), ¿Había apoyo técnico de parte de la ONGEI?
E: Con la norma anterior había muy poco apoyo técnico, a pesar de haberlo solicitado, no tuve mucha respuesta en su momento. Tuve alguna vez la visita del Sr. Frayssinet e hizo la revisión de lo que se había avanzado y tuve varias observaciones que me ayudaron en la nueva norma. Pero desde allí ya no tuve mayor apoyo de ONGEI.

Yo: ¿Qué objetivos cree que busca el Estado Peruano con la implementación de esta norma?
E: Lo que busca es fomentar el uso de los activos informáticos, tener mucho mayor cuidado sobretodo en el tratamiento de la información. Por ejemplo, ahora estamos previendo los ataques informáticos, cómo tenemos que estar preparados, qué procedimientos se deben hacer, cómo debemos actuar ante esto, cómo hacer que los servicios tecnológicos dentro de la institución no paren. Entonces, yo creo que la norma más bien nos ayuda a que todos tengamos conocimiento de cómo actuar.

Yo: ¿Qué factores cree Ud. que vienen influyendo en el Estado en la implementación de la NTP 27001?
E: Primeramente, yo creo que un factor crítico de éxito es tener el apoyo de la Alta Dirección, lo cual es básico para poder fomentar esta norma. Segundo, es que las instituciones como es la ONGEI, también brinden el apoyo, brinden las herramientas necesarias, estén al día con el tema regulatorio. Otro factor también es la motivación existente en el personal de las instituciones sobre seguridad de la información. Se ve que hay una cierta respuesta con respecto al fomento de la norma.

Yo: ¿Tiene Ud. conocimiento de normas técnicas anteriores a la NTP 27001?
E: Bueno, con respecto a normas anteriores como es la 17799 no tengo muchas referencias puesto que como te comenté, yo me inicié más con la 27001. Con respecto a la 27001, la vengo revisando, incluso estoy viendo que se relaciona con otras normas como es la 31000 de riesgos y también con COBIT

Yo: ¿Y tiene conocimiento de algún caso de éxito de alguna entidad que haya implementado la NTP 27001?
E: Me parece que INDECOPI ha tenido mayor éxito en su implementación. Sin embargo, no tengo mayor información que esté publicada en internet.

Yo: Hace poco se ha aprobado la NTP 27001:2014 ¿Cree que esto beneficiará más la implementación en el Estado?
E: Yo creo que si beneficia más la actual con respecto a la anterior. A pesar de que tiene más fases a ejecutar pero hay ciertos criterios dentro del Anexo A que, como te comenté, se integra con otras normas que la hacen más dinámica.

Respecto a la Dimensión Institucional, es decir preguntas referidas a la seguridad de la información en su institución:

Yo: ¿Cómo cree Ud. que viene beneficiando en su institución la implementación de la Norma Técnica 27001?
E: Primero, cuáles son los sistemas críticos, contar con procedimientos para la continuidad de negocios, fomentar la cultura en seguridad de la información en la institución. Además, si nos certificáramos se tendría una buena imagen.

Yo: ¿En su institución existe el apoyo de la Alta Dirección para la implementación de la NTP 27001?

E: Si existe el apoyo de la alta dirección, tanto del secretario general, como del director de tecnologías de información.

Yo: ¿Y en qué nivel o fase de la implementación incremental de la norma se encuentran?

E: Actualmente, nos encontramos en la Fase 1, que es el análisis del contexto de la Organización y la declaración del Alcance. Para ello, acabamos de enviar un documento a ONGEI para que nos preste el apoyo técnico para su revisión. Estamos a la espera de su respuesta.

Yo: ¿Cuál es el Alcance que han definido en su institución?
E: Bueno, el alcance va a comprender todos los procesos misionales que tengan que ver con las tareas que tengan que ver con el procesamiento y recopilación de información en cualquier tipo de medio sea este físico o digital.

Yo: ¿Pero ese alcance es sobre un proceso determinado?
E: Bueno, la determinación del alcance se tomó en base a que como todos los procesos tienen que ver con lo que es el procesamiento de información y los diversos servicios que brinda esta institución, culturales, por ejemplo. Entonces, todos esos servicios se enlazan y el área que lo realiza es el de TI. Por tanto, ésta termina "conversando" con todos los procesos requeridos.
Por tanto, el alcance que hemos tomado es el del área de Tecnologías de la Información, incluyendo el Data Center, además de Trámite Documentario que ya está 100% digitalizado y se tiene que ver la manera de prevenir la continuidad de los procesos ante la ocurrencia de algún desastre por ejemplo.

Yo: ¿Qué estructura organizacional tienen instalada en su institución respecto del SGSI?
E: Tenemos definido un comité de gestión del SGSI. Esto fue realizado ni bien salió la resolución de la NTP actual. Ya se han definido las personas que lo conforman y sus roles y funciones.
El comité está conformado por la Directora de OAF, el de OAJ, el Secretario General, el Director de TI y el oficial de seguridad, en este caso mi persona.
Yo: ¿Este comité se reúne periódicamente o no?
Después de su conformación, las coordinaciones las hemos realizado por correo electrónico. Las reuniones se tendrán al cierre de cada una de las fases de la implementación de la norma. Por ahora quiero que primero lo revise lo avanzado la ONGEI y después haremos la presentación a la Alta Dirección.

Yo: ¿Tienen asignado un presupuesto de forma exclusiva para la implementación del SGSI?
E: Bueno, básicamente nosotros no contamos con presupuesto. Por eso es que toda implementación que hemos realizado durante esta última gestión ha sido en base a las remuneraciones del personal. Por ejemplo, el plan estratégico que hemos hecho el año pasado no nos generó ningún gasto por que básicamente lo hemos trabajado nosotros.

Yo: ¿Tienen alguna metodología de riesgos que ya están utilizando o piensan utilizar? ¿Es propia?
E: Para la identificación de riesgos estamos utilizado una metodología propia, la cual tiene que ver con ponderaciones que nos permitan identificar los activos con los riesgos más críticos. Aunque aún no llegamos a esa fase.

Yo: ¿La Alta Dirección ha dado el apoyo necesario para el desarrollo del SGSI?
E: Bueno, el SGSI está dentro del Plan Operativo Institucional y continuamente se está notificando sobre los avances de este. Ahora, gracias a ello nos han autorizado la pre-auditoría por una consultora, el cual nos determinará el estado actual del avance del SGSI en la entidad.

Yo: ¿Cree que la Alta Dirección tiene clara la importancia de implementar el SGSI?
E: No, yo creo que la AD aún no tienen bien en claro el SGSI. Ellos tienen una idea básica de qué cosa es seguridad de la información pero muy clara todavía. Más bien dentro de poco tengo que hacer una presentación a ellos y ahí se les explicará más en detalle

Yo: ¿Ud. está de acuerdo con que el área de TI sea la encargada de implementar el SGSI?
E: Si estoy de acuerdo, ya que todos los activos se encuentran en esa área. Entonces las coordinaciones se realizan más directamente. Sin embargo, tengo entendido que el oficial de seguridad tiene que estar a nivel de la alta dirección.

Yo: ¿Cómo oficial de seguridad tienes acceso directo a la Alta Dirección?
E: No, el acceso es a través del Director de Informática.

Yo: ¿Se ha recibido alguna capacitación en SGSI en su institución?
E: No, todavía no. Pero si está programada recibir la primera capacitación dentro de dos meses dirigido al personal de la institución. La capacitación al comité se realizará dentro de un mes. Dicha capacitación lo realizará el oficial de seguridad.

Yo: ¿Y hay una cultura organizacional del SGSI en el personal de su institución?
E: El personal de esta institución actualmente no tiene una cultura organizacional en seguridad de la información, ya que como recién vamos a comenzar a enviar información sobre la implementación de la norma recién van a adquirir ese conocimiento. Tienen una idea muy básica.

Yo: ¿Hay un plan de trabajo de concientización del personal en seguridad de la información?
E: Si hay elaborado un plan que se iniciará en dos meses.

Yo: ¿Existe un programa de concientización del SGSI al personal de su institución?
E: El tema de concientización ya empieza pronto iniciándose con el envío de banners (mensajes gráficos) sobre el concepto de los que es seguridad de información y otro con la conformación de los integrantes del comité de seguridad de información. Además, estamos elaborando otro sobre el cuidado que deben tener los usuarios de la entidad con los activos informáticos por ejemplo.

Yo: ¿Y cómo se distribuyen estos banners?
E: Se distribuyen a través del correo electrónico o también a través de la intranet.

Yo: ¿Qué otros factores cree Ud. que impactan o impiden la implementación del SGSI en las instituciones de la administración pública?
E: Bueno, un factor relevante es la falta de apoyo de la Alta Dirección. Otro factor es que no estén totalmente capacitados en el SGSI. Otro factor es que no hay muchas capacitaciones por parte de ONGEI, habría que fomentarlo un poco más. Otro tema es el presupuestal para asignar a un personal especializado en seguridad de información y no a cualquier personal que no tenga conocimientos en SGSI. Otro factor que afecta también es la falta de apoyo o interés del personal de la institución en este tema. Un factor que me parece podría afectar de sobremanera es la actual transición de gobierno por los cambios de personal que podrían generarse en los altos mandos.